Refine Search

Search Results -

Terms	Documents
707.clas.	32028

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Thursday, January 26, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L30	707.clas.	32028	L30
L29	709.clas.	41731	L29
L28	709/207	1460	L28
L27	709/208	1312	L27
L26	709/209	472	L26
L25	709/201	4761	L25
L24	707/3	7882	L24
L23	707/100	7238	L23
L22	707/1	7395	L22
L21	5864683.pn.	2	L21
L20	6212553.pn.	2	L20
	DB=USPT; PLUR=YES; OP=OR		
L19	(5652789 | 5245532 | 5057935 | 5493692 | 5377354 | 5675733)![PN]	6	L19

DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR

L18	('6108688')[ABPN1,NRPN,PN,TBAN,WKU]	2	L18
L17	6108688.pn.	2	L17
L16	L10 and 713/201	13	L16
L15	L10 and 713.clas.	24	L15
L14	L10 and 701.clas.	0	L14
L13	L10 and 707.clas.	4	L13
L12	L10 and 709.clas.	7	L12
L11	L10 and 709/209	0	L11
L10	L9 and (security with rules or security near rules or security adj rules)	94	L10
L9	L7 and (deletion or delet$ or purg$ or delete) and rights	218	L9
L8	L7 and (deletion or delet$ or purg$ or delete) near rights	3	L8
L7	L6 and (user with rights or user near rights or user adj rights or user with access with rights or user near access near rights or user adj access adj rights or user with profile or user near profile or user adj profile)	332	L7
L6	L5 and (electronic with record or electronic near record or electronic adj record)	859	L6
L5	L4 and (tag or anchor)	12789	L5
L4	(electronic near mail or electronic with mail or electronic adj mail or e-mail or chat)	104077	L4
DB=USPT; PLUR=YES; OP=OR			
L3	(5797128 | 5621889 | 5197114 | 5142612 | 5845065 | 6070244 | 5355474 | 5408586 | 5440744 | 5603054 | 5579222)![PN]	11	L3
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L2	('6735701')[ABPN1,NRPN,PN,TBAN,WKU]	2	L2
L1	6735701.pn.	2	L1

END OF SEARCH HISTORY

Day : Thursday
Date: 1/26/2006

PALM INTRANET

Time: 10:04:01

Inventor Name Search Result

Your Search was:

Last Name = JACOBSON
First Name = ANDREA

Application#	Patent#	Status	Date Filed	Title	Inventor Name
10815092	Not Issued	20	03/31/2004	Network policy management and effectiveness system	JACOBSON, ANDREA M.
09104946	6735701	150	06/25/1998	NETWORK POLICY MANAGEMENT AND EFFECTIVENESS SYSTEM	JACOBSON, ANDREA M.
09175589	Not Issued	71	10/20/1998	ELECTRONIC RECORD MANAGEMENT SYSTEM	JACOBSON, ANDREA M.

Inventor Search Completed: No Records to Display.

Search Another: Inventor **Last Name** jacobson **First Name** andrea Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 09175589 **Filing Dt:** 10/20/1998 **Patent #:** NONE **Issue Dt:**

PCT #: NONE **Publication #:** NONE **Pub Dt:**

Inventor: ANDREA M. JACOBSON

Title: ELECTRONIC RECORD MANAGEMENT SYSTEM

Assignment: 1

Reel/Frame:	Received:	Recorded:	Mailed:	Pages:
009533 / 0260	10/29/1998	10/20/1998	02/17/1999	3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: JACOBSON, ANDREA M. **Exec Dt:** 10/20/1998

Assignee: VIRTUAL WORKSPACE, INC.
250 EAST SIXTH STREET, #610
ST. PAUL, MINNESOTA 55101

Correspondent: MERCHANT, GOULD ET AL.
ROBERT J. GLANCE
3100 NORWEST CENTER
90 SOUTH SEVENTH STREET
MINNEAPOLIS, MN 55402-4131

Assignment: 2

Reel/Frame:	Received:	Recorded:	Mailed:	Pages:
009957 / 0959	05/21/1999	05/17/1999	07/22/1999	3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignor: VIRTUAL WORKSPACE, LLC **Exec Dt:** 05/12/1999

Assignee: JACOBSON FAMILY HOLDINGS, LLC
P.O. BOX 53
PORTER, MINNESOTA 56280

Correspondent: MERCHANT, GOULD, SMITH, EDELL ET AL.
ROBERT J. GLANCE
3100 NORWEST CENTER
90 SOUTH SEVENTH STREET
MINNEAPOLIS, MN 55402-4131

Search Results as of: 1/26/2006 10:05:42 A.M.

If you have any comments or questions concerning the data displayed, contact OPR / Assignments at 571-272-3350
Web interface last modified: September 28, 2005

Web Results **1** - **10** of about **27,200,000** for **managing information in electronic mail <1998**. (**0.22** seconds)

Book results for **managing information in electronic mail <1998**

Managing Information Technology in ... - by Mehdi Khosrow-Pour - 1200 pages
Managing Information Technology in ... - by Stephen Burgess - 367 pages
Consumer Health Informatics - edited by Deborah Lewis, Gunther Eysenbach, Rita Kukafka, ... - 258 pages

[PDF] CAFE: A Conceptual Model for **Managing Information** in **Electronic Mail**
File Format: PDF/Adobe Acrobat
CAFE: A Conceptual Model for **Managing Information** in **Electronic Mail**. Juha Takkinen and Nahid Shahmehri. Laboratory for Intelligent **Information** Systems ...
doi.ieeecomputersociety.org/10.1109/HICSS.**1998**.648295 - Similar pages

Mailman, the GNU **Mailing** List Manager
Email Us. mailman-users@python.org · SourceForge Logo. © **1998**-2006 Free Software ...
Mailman is free software for **managing electronic mail** discussion and ...
www.gnu.org/software/**mail**man/ - 8k - Jan 24, 2006 - Cached - Similar pages

Electronic Records
Information Management Forum. Guidelines on **Managing Electronic Mail ... 1998**; **Managing Email** Effectively. 2002; New York State Use of **Electronic Mail**. ...
www.archives.state.ut.us/recmanag/**electronic**.htm - 82k - Cached - Similar pages

Recordkeeping and E-**mail** Policy: The State of Thought and the ...
Electronic Mail Guideline Task Force, **Electronic Mail** Guideline, Draft (May **1998**), p. 6. Michael JD Sutton, Document **Management** for the Enterprise: ...
www.mybestdocs.com/dwallace.html - 156k - Cached - Similar pages

Electronic Document **Management** - New Technologies in **Information** ...
New Technologies in **Information Management**. Chair's Welcoming Remarks. Day One of the **Electronic** Document **Management 1998** Conference. Tom Worthington ...
www.acs.org.au/president/**1998**/past/edm98.htm - 20k - Cached - Similar pages

Electronic and Voice **Mail**:
 A **Management** Guide for Maine State ...
Organizing and **managing e-mail** (and other files) will save space, provide more ...
Information in **electronic mail** systems regarding date and time of receipt ...
www.state.me.us/sos/arc/general/admin/**email**.htm - 36k - Cached - Similar pages

Electronic Recordkeeping > Document & File **Management** > **Electronic** ...
British Columbia - Recorded **Information Management** Manual, **Electronic Mail ... 1998**; Foundation for **Information** Technology - AITP Model **Electronic Mail** ...
www-personal.si.umich.edu/~calz/ermlinks/**email**.htm - 10k - Cached - Similar pages

Policy on **Electronic** Messages as Records

... for example, within header **information** for **electronic mail**). ... 4.1 Effective practices for **managing electronic** messages as records will help ensure ...
www.records.nsw.gov.au/ publicsector/erk/polem/messag.htm - 20k -
Cached - Similar pages

PADI - **Email**
NARA: **Electronic Information Management** Standards NARA (National Archives and Records Administration) (Last Updated: 1 Jul **1998**) (United States of America) ...
www.nla.gov.au/padi/topics/47.html - 39k - Cached - Similar pages

TR: **Managing Electronic** Records '98 Conference+, Chicago, Nov 2-4 ...
TR: **Managing Electronic** Records '98 Conference+, Chicago, Nov 2-4, **1998** ... 0) 2.650.53.67 - **email**:ddevriese@admin.ulb.ac.be http://www.ulb.ac.be/ ...
www.asap.unimelb.edu.au/asa/stama/**mail**/msg00222.html - 11k - Cached - Similar pages

Try your search again on Google Book Search

Gooooooooooogle ►
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

managing information in electronic n Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

IP.com PriorArtDatabase

Secu

January 26, 2006 USPTO

Search

- Full Text
- Concept
- Document ID
- Recent Disclosures

Other

- Prior Art Home
- Support
- Logout

Fingerprint Lookup

Lookup

Displaying records #1 through 10 out of 500
(search stopped at 500 hits)

Result # 1 Relevance:

FYI on where to start: A bibliography of internetworking information

1990-08-01 IPCOM000001988D Englisl

The intent of this bibliography is to offer a representative collection of resources of infc will help the reader become familiar with the concepts of internetworking. It is meant t place for further research. There are references to other ...

Result # 2 Relevance:

Internet Users' Glossary (RFC1392)

1993-01-01 IPCOM000002216D Englisl

There are many networking glossaries in existence. This glossary concentrates on term specific to the Internet. Naturally, there are entries for some basic terms and acronym entries refer to them.

Result # 3 Relevance:

Internet Users' Glossary (RFC1983)

1996-08-01 IPCOM000004200D Englisl

There are many networking glossaries in existence. This glossary concentrates on term specific to the Internet. Naturally, there are entries for some basic terms and acronym entries refer to them.

Result # 4 Relevance:

BEEPER - Electronic MAIL and Reminder Paging System

1985-04-01 IPCOM000063659D Englisl

BEEPER is an easy-to-use paging system for electronic mail users. Once activated, BEE electronic mail users to be contacted at a forwarding location (CPU) if electronic mail is it is time for a PROFS reminder. (PROFS is IBM's Professional Office ...

Result # 5 Relevance:

Privacy enhancement for Internet electronic mail: Part I: Message en and authentication procedures (RFC1040)

1988-01-01 IPCOM000001846D Englisl

STATUS OF THIS MEMO

Result # 6 Relevance:

Privacy enhancement for Internet electronic mail: Part I: Message en and authentication procedures (RFC0989)

1987-02-01 IPCOM000004986D Englisl

STATUS OF THIS MEMO

Result # 7 Relevance:

Privacy enhancement for Internet electronic mail: Part I - message e and authentication procedures (RFC1113)

1989-08-01 IPCOM000001923D Englisl

IP.com PriorArtDatabase

Secur

January 26, 2006 USPTO

Search

- Full Text
- Concept
- Document ID
- Recent Disclosures

Other

- Prior Art Home
- Support
- Logout

Fingerprint Lookup

Lookup

Displaying records #1 through 10 out of 500
(search stopped at 500 hits)

Result # 1 Relevance:

FYI on where to start: A bibliography of internetworking information

1990-08-01 IPCOM000001988D Englisl

The intent of this bibliography is to offer a representative collection of resources of infc will help the reader become familiar with the concepts of internetworking. It is meant t place for further research. There are references to other ...

Result # 2 Relevance:

Internet Users' Glossary (RFC1392)

1993-01-01 IPCOM000002216D Englisl

There are many networking glossaries in existence. This glossary concentrates on term specific to the Internet. Naturally, there are entries for some basic terms and acronym entries refer to them.

Result # 3 Relevance:

Internet Users' Glossary (RFC1983)

1996-08-01 IPCOM000004200D Englisl

There are many networking glossaries in existence. This glossary concentrates on term specific to the Internet. Naturally, there are entries for some basic terms and acronym entries refer to them.

Result # 4 Relevance:

BEEPER - Electronic MAIL and Reminder Paging System

1985-04-01 IPCOM000063659D Englisl

BEEPER is an easy-to-use paging system for electronic mail users. Once activated, BEE electronic mail users to be contacted at a forwarding location (CPU) if electronic mail is it is time for a PROFS reminder. (PROFS is IBM's Professional Office ...

Result # 5 Relevance:

Privacy enhancement for Internet electronic mail: Part I: Message en and authentication procedures (RFC1040)

1988-01-01 IPCOM000001846D Englisl

STATUS OF THIS MEMO

Result # 6 Relevance:

Privacy enhancement for Internet electronic mail: Part I: Message en and authentication procedures (RFC0989)

1987-02-01 IPCOM000004986D Englisl

STATUS OF THIS MEMO

Result # 7 Relevance:

Privacy enhancement for Internet electronic mail: Part I - message e and authentication procedures (RFC1113)

1989-08-01 IPCOM000001923D Englisl

STATUS OF THIS MEMO

Result # 8 Relevance:

Replaceable Pin Arrays for Detack and Pre-Clean Corotrons

15-Aug-2003 IPCOM000018826D Englisl

Pin arrays are fragile. Any deformation to the part, via bent pins or deformed surface, inefficiency in the system. The replaceable pin will be sandwiched between two plastic secured by snap fitting together. This will now enable ease of handling of ...

Result # 9 Relevance:

Guide to Network Resource Tools (RFC1580)

1994-03-01 IPCOM000002414D Englisl

As the worldwide academic computer network grows and expands far beyond its previc the resources and services available on the network evolve and multiply at a dizzying r user is hardpressed to keep up with this explosive growth. Fortunately, a ...

Result # 10 Relevance:

FYI on Questions and Answers Answers to Commonly asked "New In Questions (RFC1325)

1992-05-01 IPCOM000002147D Englisl

This FYI RFC is one of two FYI's called, "Questions and Answers" (Q/A), produced by tl Services Working Group of the Internet Engineering Task Force (IETF). The goal is to c most commonly asked questions and answers in the Internet.

Displaying page 1 of 50 << FIRST | < BACK | NEXT > | LAST >>

Search query: electronic mail

New search | Modify this search | Search within current results

IEEE Xplore® RELEASE 2.1

Welcome United States Patent and Trademark Office

Thu, 26 Jan 2006, 1:56:48 PM EST

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Search Query Display

[redacted] [redacted]

Recent Search Queries

#1	(electronic mail<in>metadata)
#2	(electronic mail<in>metadata)
#3	(electronic mail<in>metadata)
#4	(electronic mail<in>metadata)
#5	((electronic mail<in>metadata) <and> (network<in>metadata))<and> (security<in>metadata)
#6	((electronic mail<in>metadata) <and> (network<in>metadata))<and> (security<in>metadata)
#7	((electronic mail<in>metadata) <and> (network<in>metadata))<and> (security<in>metadata)
#8	((microsoft outlook<in>metadata) <and> (electronic mail<in>metadata))
#9	(microsoft outlook<in>metadata)
#10	(lotus notes<in>metadata)

[redacted]

Results for "(lotus notes<in>metadata)"

e-mail

Your search matched **53** of **1306777** documents.
A maximum of **53** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(lotus notes<in>metadata)

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select **Article Information** **View: 1-**

1. **Using control theory to achieve service level objectives in performance n**
Parekh, S.; Gandhi, N.; Hellerstein, J.; Tilbury, D.; Jayram, T.; Bigus, J.;
Integrated Network Management Proceedings, 2001 IEEE/IFIP International S
14-18 May 2001 Page(s):841 - 854
Digital Object Identifier 10.1109/INM.2001.918084
AbstractPlus | Full Text: PDF(760 KB) **IEEE CNF**

2. **Expert system and Lotus Notes applications for retrieval of problem-solv and information**
Kiger, R.;
Professional Communication Conference, 1996. IPCC '96 Proceedings. 'Comn Fast Track'., International
18-20 Sept. 1996 Page(s):344 - 350
Digital Object Identifier 10.1109/IPCC.1996.552704
AbstractPlus | Full Text: PDF(412 KB) **IEEE CNF**

3. **Did you ever have to make up your mind? What Notes users do when fac security decision**
Zurko, M.E.; Kaufman, C.; Spanbauer, K.; Bassett, C.;
Computer Security Applications Conference, 2002. Proceedings. 18th Annual
9-13 Dec. 2002 Page(s):371 - 381
Digital Object Identifier 10.1109/CSAC.2002.1176309
AbstractPlus | Full Text: PDF(534 KB) **IEEE CNF**

4. **Managing collaborative knowledge-based teams: the use and misuse of c supported technologies**
Sena, J.; Shani, A.B.;
Management of Engineering and Technology, 2001. PICMET '01. Portland Inte Conference on
Volume 1, 29 July-2 Aug. 2001 Page(s):112 vol.1
Digital Object Identifier 10.1109/PICMET.2001.951818
AbstractPlus | Full Text: PDF(66 KB) **IEEE CNF**

5. **Feedback control of a Lotus Notes server: modeling and control design**
Gandhi, N.; Tilbury, D.M.; Parekh, S.; Hellerstein, J.;
American Control Conference, 2001. Proceedings of the 2001
Volume 4, 25-27 June 2001 Page(s):3000 - 3005 vol.4
Digital Object Identifier 10.1109/ACC.2001.946372

AbstractPlus | Full Text: PDF(504 KB) **IEEE CNF**

☐ 6. **Application of a comprehensive Product Environmental Profile system to environment**
Ching, S.; Jacques, M.; Kirby, J.R.; Mann, T.;
Electronics and the Environment, 1999. ISEE -1999. Proceedings of the 1999 I Symposium on
11-13 May 1999 Page(s):82 - 86
Digital Object Identifier 10.1109/ISEE.1999.765853
AbstractPlus | Full Text: PDF(476 KB) **IEEE CNF**

☐ 7. **Supporting a software engineering course with Lotus Notes**
Schoenig, S.;
Software Engineering: Education and Practice, 1998. Proceedings. 1998 Interr Conference
26-29 Jan. 1998 Page(s):304 - 311
Digital Object Identifier 10.1109/SEEP.1998.707664
AbstractPlus | Full Text: PDF(168 KB) **IEEE CNF**

☐ 8. **Supporting distributed corporate planning through new coordination tecl**
Lei Yu; Stanoevska, K.; Schmid, B.;
Database and Expert Systems Applications, 1998. Proceedings. Ninth Internat on
26-28 Aug. 1998 Page(s):559 - 565
Digital Object Identifier 10.1109/DEXA.1998.707457
AbstractPlus | Full Text: PDF(128 KB) **IEEE CNF**

☐ 9. **Experiences from the employment of workflow management systems in t sector**
Nikolaidou, M.; Anagnostopoulos, D.;
Database and Expert Systems Applications, 1998. Proceedings. Ninth Internat on
26-28 Aug. 1998 Page(s):759 - 764
Digital Object Identifier 10.1109/DEXA.1998.707493
AbstractPlus | Full Text: PDF(216 KB) **IEEE CNF**

☐ 10. **A groupware benchmark based on Lotus Notes**
Moore, K.; Peterson, M.;
Data Engineering, 1996. Proceedings of the Twelfth International Conference
26 Feb.-1 March 1996 Page(s):500 - 507
Digital Object Identifier 10.1109/ICDE.1996.492200
AbstractPlus | Full Text: PDF(588 KB) **IEEE CNF**

☐ 11. **Lotus Notes and collaboration: le plus c,a change**
Vandenbosch, B.; Ginzberg, M.J.;
System Sciences, 1996., Proceedings of the Twenty-Ninth Hawaii Internationa
Volume 3, 3-6 Jan. 1996 Page(s):61 - 71 vol.3
Digital Object Identifier 10.1109/HICSS.1996.493177
AbstractPlus | Full Text: PDF(860 KB) **IEEE CNF**

☐ 12. **Enhancing Lotus Notes for carrier grade hosting**
Cummings, P.;
Compcon '95.'Technologies for the Information Superhighway', Digest of Pape
5-9 March 1995 Page(s):488
Digital Object Identifier 10.1109/CMPCON.1995.512427
AbstractPlus | Full Text: PDF(44 KB) **IEEE CNF**

☐ 13. **Facilitating knowledge creation with GroupWare: a case study of a knowl**

firm
Robertson, M.; Sorensen, C.; Swan, J.;
System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International (
Jan 4-7 2000 Page(s):9 pp.

AbstractPlus | Full Text: PDF(84 KB) **IEEE CNF**

☐ 14. **Implementing reuse with RAD tools' native objects**
Zubeck, J.C.;
Computer
Volume 30, Issue 10, Oct. 1997 Page(s):60 - 65
Digital Object Identifier 10.1109/2.625308

AbstractPlus | References | Full Text: PDF(112 KB) **IEEE JNL**

☐ 15. **The communication characteristics of virtual teams: a case study**
Suchan, J.; Hayzak, G.;
Professional Communication, IEEE Transactions on
Volume 44, Issue 3, Sept. 2001 Page(s):174 - 186
Digital Object Identifier 10.1109/47.946463

AbstractPlus | References | Full Text: PDF(72 KB) **IEEE JNL**

☐ 16. **Presence technology: more than just instant messaging**
Vaughan-Nichols, S.J.;
Computer
Volume 36, Issue 10, Oct. 2003 Page(s):11 - 13
Digital Object Identifier 10.1109/MC.2003.1236463

AbstractPlus | Full Text: PDF(296 KB) **IEEE JNL**

☐ 17. **Knowledge management for engineers**
Derby, C.;
Integration of Knowledge Intensive Multi-Agent Systems, 2003. International C
30 Sept.-4 Oct. 2003 Page(s):760 - 765
Digital Object Identifier 10.1109/KIMAS.2003.1245133

AbstractPlus | Full Text: PDF(511 KB) **IEEE CNF**

☐ 18. **Workflow interoperability using extensible markup language (XML)**
Dahalin, Z.M.; Wahid, J.;
Research and Development, 2002. SCOReD 2002. Student Conference on
16-17 July 2002 Page(s):513 - 516
Digital Object Identifier 10.1109/SCORED.2002.1033171

AbstractPlus | Full Text: PDF(394 KB) **IEEE CNF**

☐ 19. **Using of an e-learning tool at the University of Klagenfurt**
Wickl, J.;
Management of Engineering and Technology, 2001. PICMET '01. Portland Int(
Conference on
Volume 1, 29 July-2 Aug. 2001 Page(s):330 vol.1
Digital Object Identifier 10.1109/PICMET.2001.952214

AbstractPlus | Full Text: PDF(36 KB) **IEEE CNF**

☐ 20. **Toward inclusive dialogue: participation and interaction in face-to-face a**
mediated discussions
Balthazard, P.A.; Potter, R.E.;
System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International (
Jan 4-7 2000 Page(s):10 pp.

AbstractPlus | Full Text: PDF(84 KB) **IEEE CNF**

☐ 21. **Using groupware for international collaborative learning**
Clear, T.; Daniels, M.;

Frontiers in Education Conference, 2000. FIE 2000. 30th Annual
Volume 1, 18-21 Oct. 2000 Page(s):F1C/18 - F1C/23 vol.1
Digital Object Identifier 10.1109/FIE.2000.897682

AbstractPlus | Full Text: PDF(488 KB) **IEEE CNF**

☐ **22. A first report on a new technique to model workflow systems**
Thom, L.H.; Scheidt, N.; Molz, K.W.;
Software Methods and Tools, 2000. SMT 2000. Proceedings. International Coı
6-9 Nov. 2000 Page(s):223 - 229
Digital Object Identifier 10.1109/SWMT.2000.890438

AbstractPlus | Full Text: PDF(468 KB) **IEEE CNF**

☐ **23. ETE: a customizable approach to measuring end-to-end response times ;**
components in distributed systems
Hellerstein, J.L.; Maccabee, M.M.; Mills, W.N., III; Turek, J.J.;
Distributed Computing Systems, 1999. Proceedings. 19th IEEE International C
31 May-4 June 1999 Page(s):152 - 162
Digital Object Identifier 10.1109/ICDCS.1999.776516

AbstractPlus | Full Text: PDF(1944 KB) **IEEE CNF**

☐ **24. Innovative concepts for configuring shared workspaces through visual p**
Duecker, M.; Mueller, W.; Rubart, J.;
System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii In
Conference on
Volume Track8, 5-8 Jan. 1999 Page(s):9 pp.
Digital Object Identifier 10.1109/HICSS.1999.773046

AbstractPlus | Full Text: PDF(240 KB) **IEEE CNF**

☐ **25. An asynchronous group decision support system study for intelligent mı**
decision making
Cao, P.P.; Burstein, F.V.;
System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii In
Conference on
Volume Track1, 5-8 Jan. 1999 Page(s):9 pp.
Digital Object Identifier 10.1109/HICSS.1999.772713

AbstractPlus | Full Text: PDF(100 KB) **IEEE CNF**

[redacted] **View: 1-**

Help Contact Us Privacy & :

Indexed by Inspec

Home | Login | Logout | Access Information

IEEE Xplore RELEASE 2.1

Welcome United States Patent and Trademark Office

Advanced Search

BROWSE | SEARCH | IEEE XPLORE GUIDE

OPTION 1
Enter keywords or phrases, select fields, and select operators | Help

electronic mail in All Fields

AND network in All Fields

AND security in All Fields

» Note: If you use all three search boxes, the entries in the first two boxes take precedence over the entry in the third box.

OPTION 2
Enter keywords, phrases, or a Boolean expression | Help

» Note: You may use the search operators <and> or <or> without the start and end brackets <>.

» Learn more about Field Codes, Search Examples, and Search Operators

» Publications

- Select publications
- IEEE Periodicals
- IEE Periodicals
- IEEE Conference
- IEE Conference P
- IEEE Standards

» Other Resources (Availat

- IEEE Books

» Select date range

- Search latest content u
- From year All
- to Present

» Display Format

Citation | Citatio

» Organize results

Maximum 100

Display 25 resı

Sort by Relevance

In Descending

Help Contact Us

Indexed by Inspec

Results for "(electronic mail<in>metadata)"
Your search matched **820** of **1306777** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

e-mail

» Search Options

View Session History

New Search

Modify Search

(electronic mail<in>metadata)

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information **View: 1-25** | 26-5

1. **Electronic mail-E-mail at work**
Perry, T.S.;
Spectrum, IEEE
Volume 29, Issue 10, Oct. 1992 Page(s):24 - 28
Digital Object Identifier 10.1109/6.158629
AbstractPlus | Full Text: PDF(732 KB) **IEEE JNL**

2. **"Media-on-demand" multimedia electronic mail: a tool for collaboration o**
Tsoi, K.N.; Rahman, S.M.;
High Performance Distributed Computing, 1996., Proceedings of 5th IEEE Inte
Symposium on
6-9 Aug. 1996 Page(s):121 - 126
AbstractPlus | Full Text: PDF(948 KB) **IEEE CNF**

3. **Requirement analysis for next generation electronic mail systems**
Hui, S.; Foo, S.; Daroy, C.J.;
Networks, 1993. International Conference on Information Engineering '93. 'Cor
Networks for the Year 2000', Proceedings of IEEE Singapore International Cor
Volume 2, 6-11 Sept. 1993 Page(s):735 - 739 vol.2
Digital Object Identifier 10.1109/SICON.1993.515685
AbstractPlus | Full Text: PDF(432 KB) **IEEE CNF**

4. **Electronic mail, information management and organizational culture**
McMurdo, G.;
Human Factors in Electronic Mail and Conferencing Systems, IEE Colloquium
3 Feb 1989 Page(s):3/1 - 3/6
AbstractPlus | Full Text: PDF(360 KB) **IEE CNF**

5. **Trial and survey of the use of electronic mail for disseminating a library n**
Youngman, F.M.;
Human Factors in Electronic Mail and Conferencing Systems, IEE Colloquium
3 Feb 1989 Page(s):2/1 - 2/4
AbstractPlus | Full Text: PDF(264 KB) **IEE CNF**

6. **Authenticating multicast Internet electronic mail messages using a bidire insecure**
Mitchell, C.J.;

Computers, IEEE Transactions on
Volume 41, Issue 4, April 1992 Page(s):505 - 507
Digital Object Identifier 10.1109/12.135563
AbstractPlus | Full Text: PDF(288 KB) **IEEE JNL**

☐ 7. **X.400 message handling system: the remote user agent**
Rotzal, P.H.;
Military Communications Conference, 1995. MILCOM '95, Conference Record,
Volume 2, 5-8 Nov. 1995 Page(s):433 - 437 vol.2
Digital Object Identifier 10.1109/MILCOM.1995.483504
AbstractPlus | Full Text: PDF(348 KB) **IEEE CNF**

☐ 8. **Electronic mail-forces for social change**
Perry, T.S.;
Spectrum, IEEE
Volume 29, Issue 10, Oct. 1992 Page(s):30 - 32
Digital Object Identifier 10.1109/6.158631
AbstractPlus | Full Text: PDF(388 KB) **IEEE JNL**

☐ 9. **Experiences with electronic and voice mail**
Hayne, S.C.; Smith, C.A.P.;
System Sciences, 1996., Proceedings of the Twenty-Ninth Hawaii Internationa
Volume 3, 3-6 Jan. 1996 Page(s):102 - 111 vol.3
Digital Object Identifier 10.1109/HICSS.1996.493181
AbstractPlus | Full Text: PDF(912 KB) **IEEE CNF**

☐ 10. **Graphical knowledge based electronic mail system (GKBEMS)**
Kantardzic, M.; Milicic, N.; Jusupovic, U.;
Electrotechnical Conference, 1991. Proceedings., 6th Mediterranean
22-24 May 1991 Page(s):1165 - 1168 vol.2
Digital Object Identifier 10.1109/MELCON.1991.162048
AbstractPlus | Full Text: PDF(240 KB) **IEEE CNF**

☐ 11. **Securing electronic mail systems**
Serenelli, B.; Leisher, T.;
Military Communications Conference, 1992. MILCOM '92, Conference Record
'Communications - Fusing Command, Control and Intelligence'., IEEE
11-14 Oct. 1992 Page(s):677 - 680 vol.2
Digital Object Identifier 10.1109/MILCOM.1992.244144
AbstractPlus | Full Text: PDF(196 KB) **IEEE CNF**

☐ 12. **A multimedia electronic mail system on a heterogeneous environment**
Hui, S.C.; Foo, S.; Leong, P.C.; Daroy, C.J.;
TENCON '93. Proceedings. Computer, Communication, Control and Power Er
IEEE Region 10 Conference on
Issue 0, Part 10000, 19-21 Oct. 1993 Page(s):61 - 64 vol.1
Digital Object Identifier 10.1109/TENCON.1993.319928
AbstractPlus | Full Text: PDF(284 KB) **IEEE CNF**

☐ 13. **Multimedia electronic mail on X.400: a pragmatic approach**
Carrier, S.; Georganas, N.D.;
Multimedia Communications, 1994. MULTIMEDIA '94., 5th IEEE COMSOC Int
Workshop on
16-19 May 1994 Page(s):5/4/1 - 5/4/6
Digital Object Identifier 10.1109/IWMC.1994.601223
AbstractPlus | Full Text: PDF(492 KB) **IEEE CNF**

14. **MEmail: a distributed multimedia electronic mail system**

☐ Daroy, C.J.; Hui, S.C.; Foo, S.;
Singapore ICCS '94. Conference Proceedings.
Volume 3, 14-18 Nov. 1994 Page(s):981 - 985 vol.3
Digital Object Identifier 10.1109/ICCS.1994.474257
AbstractPlus | Full Text: PDF(344 KB) **IEEE CNF**

☐ **15. Multi-media electronic mail facilities: a user-interface design case study**
Barker, P.;
Human Factors in Electronic Mail and Conferencing Systems, IEE Colloquium
3 Feb 1989 Page(s):7/1 - 7/5
AbstractPlus | Full Text: PDF(300 KB) **IEE CNF**

☐ **16. Internetworking with the Power Globe remailer**
Ramesh, V.C.; Heydt, G.T.;
Computer Applications in Power, IEEE
Volume 8, Issue 3, July 1995 Page(s):36 - 39
Digital Object Identifier 10.1109/67.392025
AbstractPlus | Full Text: PDF(364 KB) **IEEE JNL**

☐ **17. Forming mental models in learning operating procedures for terminal eq**
Matsuo, N.; Matsui, H.; Tokunaga, Y.;
Selected Areas in Communications, IEEE Journal on
Volume 9, Issue 4, May 1991 Page(s):548 - 554
Digital Object Identifier 10.1109/49.81947
AbstractPlus | Full Text: PDF(492 KB) **IEEE JNL**

☐ **18. The effect of management and social interaction on the intra-firm diffusic mail systems**
Astebro, T.;
Engineering Management, IEEE Transactions on
Volume 42, Issue 4, Nov. 1995 Page(s):319 - 331
Digital Object Identifier 10.1109/17.482082
AbstractPlus | Full Text: PDF(1484 KB) **IEEE JNL**

☐ **19. Department of Defense e-mail policy and government-wide e-mail initiati**
Grant, P.; Tall, A.M.;
Military Communications Conference, 1995. MILCOM '95, Conference Record
Volume 3, 5-8 Nov. 1995 Page(s):972 - 976 vol.3
Digital Object Identifier 10.1109/MILCOM.1995.483498
AbstractPlus | Full Text: PDF(536 KB) **IEEE CNF**

☐ **20. Privacy enhanced electronic mail**
Casey, T.J.; Wilbur, S.R.;
Aerospace Computer Security Applications Conference, 1988., Fourth
12-16 Dec. 1988 Page(s):16 - 21
Digital Object Identifier 10.1109/ACSAC.1988.113409
AbstractPlus | Full Text: PDF(500 KB) **IEEE CNF**

☐ **21. Electronic mail, social presence and information richness**
Kydd, C.T.; Ferry, D.L.;
System Sciences, 1992. Proceedings of the Twenty-Fifth Hawaii International
Volume iv, 7-10 Jan. 1992 Page(s):380 - 391 vol.4
Digital Object Identifier 10.1109/HICSS.1992.183367
AbstractPlus | Full Text: PDF(708 KB) **IEEE CNF**

☐ **22. Protocol design for integrity protection**
Stubblebine, S.G.; Gligor, V.D.;
Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer S

Symposium on
24-26 May 1993 Page(s):41 - 53
Digital Object Identifier 10.1109/RISP.1993.287644

AbstractPlus | Full Text: PDF(1060 KB) **IEEE CNF**

☐ **23. Broadband applications and services of public switched networks**
Punj, V.;
Consumer Electronics, IEEE Transactions on
Volume 35, Issue 2, May 1989 Page(s):106 - 112
Digital Object Identifier 10.1109/30.24665

AbstractPlus | Full Text: PDF(564 KB) **IEEE JNL**

☐ **24. Graphical correspondence in electronic-mail networks using personal co**
Arnbak, J.C.; Bons, J.H.; Vieven, J.W.;
Selected Areas in Communications, IEEE Journal on
Volume 7, Issue 2, Feb. 1989 Page(s):257 - 267
Digital Object Identifier 10.1109/49.17696

AbstractPlus | Full Text: PDF(812 KB) **IEEE JNL**

☐ **25. A practical adaptive image compression technique using visual criteria f transmission with electronic mail**
Seitz, P.; Lang, G.K.;
Communications, IEEE Transactions on
Volume 38, Issue 7, July 1990 Page(s):947 - 949
Digital Object Identifier 10.1109/26.57511

AbstractPlus | Full Text: PDF(344 KB) **IEEE JNL**

View: 1-25 | 26-5

Help Contact Us Privacy & :

Indexed by Inspec

Results for "((electronic mail<in>metadata) <and> (network<in>metadata))<and> (sec..." e-mail
Your search matched **61** of **1306777** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((electronic mail<in>metadata) <and> (network<in>metadata))<and> (security<in

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information **View: 1-**

☐ 1. **Securing electronic mail systems**
Serenelli, B.; Leisher, T.;
Military Communications Conference, 1992. MILCOM '92, Conference Record. - Fusing Command, Control and Intelligence'., IEEE
11-14 Oct. 1992 Page(s):677 - 680 vol.2
Digital Object Identifier 10.1109/MILCOM.1992.244144
AbstractPlus | Full Text: PDF(196 KB) **IEEE CNF**

☐ 2. **Trials of wireless, secure electronic mail**
Smith, D.R.; Simon, S.D.; Cautilli, L.E.;
Personal Communications, IEEE [see also IEEE Wireless Communications]
Volume 2, Issue 4, Aug. 1995 Page(s):28 - 33
Digital Object Identifier 10.1109/98.403455
AbstractPlus | Full Text: PDF(660 KB) **IEEE JNL**

☐ 3. **A perspective on computer progress in the last five years**
Wilkes, M.V.;
Computing & Control Engineering Journal
Volume 1, Issue 5, Sept. 1990 Page(s):201 - 208
AbstractPlus | Full Text: PDF(944 KB) **IEE JNL**

☐ 4. **SMMM-a Secure MultiMedia Mail system**
De Moura, M.S.A.; De Souza Filho, G.L.; Batista, T.V.; Soares, L.F.G.;
Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference
Volume 3, 30 July-2 Aug. 2000 Page(s):1501 - 1504 vol.3
Digital Object Identifier 10.1109/ICME.2000.871052
AbstractPlus | Full Text: PDF(584 KB) **IEEE CNF**

☐ 5. **Information security services and standards for telecommunications in A**
Claassen, G.J.; Kuhn, G.J.; Penzhorn, W.T.;
AFRICON '92 Proceedings., 3rd AFRICON Conference
22-24 Sept. 1992 Page(s):33 - 36
Digital Object Identifier 10.1109/AFRCON.1992.624412
AbstractPlus | Full Text: PDF(388 KB) **IEEE CNF**

☐ 6. **Multiple protocol network integration: a case study in internetworking wi**
Pappa, S.; Sethi, S.; Tan, J.;

Local Computer Networks, 1992. Proceedings., 17th Conference on
13-16 Sept. 1992 Page(s):560 - 567
Digital Object Identifier 10.1109/LCN.1992.228143

AbstractPlus | Full Text: PDF(528 KB) **IEEE CNF**

☐ 7. **Development of a network model for the total health care management o**
environment
Nakagawa, S.; Kimura, M.; Chou, H.; Yamamoto, A.; Sakamoto, T.; Itokawa, Y
Sato, T.; Kimura, I.;
Multimedia Communications, 1994. MULTIMEDIA '94., 5th IEEE COMSOC Int
Workshop on
16-19 May 1994 Page(s):5/2/1 - 5/2/4
Digital Object Identifier 10.1109/IWMC.1994.601221

AbstractPlus | Full Text: PDF(508 KB) **IEEE CNF**

☐ 8. **Applications of information networks**
Licklider, J.C.R.; Vezza, A.;
Proceedings of the IEEE
Volume 66, Issue 11, Nov. 1978 Page(s):1330 - 1346

AbstractPlus | Full Text: PDF(2326 KB) **IEEE JNL**

☐ 9. **Establishment and use of a teleconsultation network in ophthalmology**
Zahlmann, G.; Kluthe, S.; Obermaier, M.; Mertz, M.; Mann, G.;
Engineering in Medicine and Biology society, 1997. Proceedings of the 19th A
Conference of the IEEE
Volume 2, 30 Oct.-2 Nov. 1997 Page(s):924 - 927 vol.2
Digital Object Identifier 10.1109/IEMBS.1997.757821

AbstractPlus | Full Text: PDF(276 KB) **IEEE CNF**

☐ 10. **Using type enforcement to assure a configurable guard**
Greve, P.; Hoffman, J.; Smith, R.E.;
Computer Security Applications Conference, 1997. Proceedings., 13th Annual
8-12 Dec. 1997 Page(s):146 - 154
Digital Object Identifier 10.1109/CSAC.1997.646187

AbstractPlus | Full Text: PDF(712 KB) **IEEE CNF**

☐ 11. **Secure official document mail systems for office automation**
Chung-Huang Yang; So-Lin Yen; Hwang David Liu; Kuei Liu; Bor-Shenn Jeng;
Min-Shin Chang; Yu-Ling Cheng; Jo-Ling Liang; Don-Min Shien;
Security Technology, 1997. Proceedings. The Institute of Electrical and Electr
31st Annual 1997 International Carnahan Conference on
15-17 Oct. 1997 Page(s):161 - 164
Digital Object Identifier 10.1109/CCST.1997.626262

AbstractPlus | Full Text: PDF(276 KB) **IEEE CNF**

☐ 12. **Proxies for anonymous routing**
Reed, M.G.; Syverson, P.F.; Goldschlag, D.M.;
Computer Security Applications Conference, 1996., 12th Annual
9-13 Dec. 1996 Page(s):95 - 104
Digital Object Identifier 10.1109/CSAC.1996.569678

AbstractPlus | Full Text: PDF(920 KB) **IEEE CNF**

☐ 13. **IDUP and SPKM: developing public-key-based APIs and mechanisms for**
security services
Adams, C.;
Network and Distributed System Security, 1996., Proceedings of the Symposi
22-23 Feb. 1996 Page(s):128 - 135
Digital Object Identifier 10.1109/NDSS.1996.492419

AbstractPlus | Full Text: PDF(724 KB) **IEEE CNF**

☐ **14. Defense Message System overview**
Clarke, T.; DeLoria, W.; Tall, A.M.;
Military Communications Conference, 1995. MILCOM '95, Conference Record
Volume 3, 5-8 Nov. 1995 Page(s):957 - 961 vol.3
Digital Object Identifier 10.1109/MILCOM.1995.483445
AbstractPlus | Full Text: PDF(516 KB) **IEEE CNF**

☐ **15. An architecture for a mobile OSI mail access system**
Cole, R.; Burns, J.;
Selected Areas in Communications, IEEE Journal on
Volume 7, Issue 2, Feb. 1989 Page(s):249 - 256
Digital Object Identifier 10.1109/49.17695
AbstractPlus | Full Text: PDF(736 KB) **IEEE JNL**

☐ **16. Security-enhanced mailing lists**
Herfert, M.;
Network, IEEE
Volume 11, Issue 3, May-June 1997 Page(s):30 - 33
Digital Object Identifier 10.1109/65.587047
AbstractPlus | Full Text: PDF(440 KB) **IEEE JNL**

☐ **17. Anonymous connections and onion routing**
Reed, M.G.; Syverson, P.F.; Goldschlag, D.M.;
Selected Areas in Communications, IEEE Journal on
Volume 16, Issue 4, May 1998 Page(s):482 - 494
Digital Object Identifier 10.1109/49.668972
AbstractPlus | References | Full Text: PDF(124 KB) **IEEE JNL**

☐ **18. Talk of the town [e-mail]**
Thomas, B.;
Internet Computing, IEEE
Volume 3, Issue 6, Nov.-Dec. 1999 Page(s):85 - 88
Digital Object Identifier 10.1109/4236.807017
AbstractPlus | Full Text: PDF(224 KB) **IEEE JNL**

☐ **19. Support vector machines for spam categorization**
Drucker, H.; Donghui Wu; Vapnik, V.N.;
Neural Networks, IEEE Transactions on
Volume 10, Issue 5, Sept. 1999 Page(s):1048 - 1054
Digital Object Identifier 10.1109/72.788645
AbstractPlus | References | Full Text: PDF(132 KB) **IEEE JNL**

☐ **20. Continuous media e-mail on the Internet: infrastructure inadequacies an(solution**
Turner, D.A.; Ross, K.W.;
Network, IEEE
Volume 14, Issue 4, July-Aug. 2000 Page(s):30 - 37
Digital Object Identifier 10.1109/65.855477
AbstractPlus | Full Text: PDF(788 KB) **IEEE JNL**

☐ **21. Invasive software, who's inside your computer**
Lawton, G.;
Computer
Volume 35, Issue 7, July 2002 Page(s):15 - 18
Digital Object Identifier 10.1109/MC.2002.1016895
AbstractPlus | Full Text: PDF(331 KB) **IEEE JNL**

22. **Merry christma: an early network worm**
Capek, P.G.; Chess, D.M.; White, S.R.; Fedeli, A.;
Security & Privacy Magazine, IEEE
Volume 1, Issue 5, Sept.-Oct. 2003 Page(s):26 - 34
Digital Object Identifier 10.1109/MSECP.2003.1236232
AbstractPlus | References | Full Text: PDF(500 KB) **IEEE JNL**

23. **Collaborative testing & support via the Internet**
Berk, K.J.; Wille, K.F.;
Aerospace and Electronic Systems Magazine, IEEE
Volume 18, Issue 6, June 2003 Page(s):25 - 29
Digital Object Identifier 10.1109/MAES.2003.1209587
AbstractPlus | References | Full Text: PDF(461 KB) **IEEE JNL**

24. **On the evolution of Internet technologies**
Cerf, V.G.;
Proceedings of the IEEE
Volume 92, Issue 9, Sep 2004 Page(s):1360 - 1370
Digital Object Identifier 10.1109/JPROC.2004.832974
AbstractPlus | References | Full Text: PDF(216 KB) | Full Text: HTML **IEEE .**

25. **Flaws in an e-mail protocol of Sun, Hsieh, and Hwang**
Dent, A.W.;
Communications Letters, IEEE
Volume 9, Issue 8, Aug 2005 Page(s):718 - 719
Digital Object Identifier 10.1109/LCOMM.2005.1496593
AbstractPlus | Full Text: PDF(129 KB) **IEEE JNL**

[redacted] **View: 1-**

Help Contact Us Privacy & :

Indexed by Inspec

IEEE Region 10 Conference on Computer and Communication Systems, September 1990, Hong Kong

COMPOUND DOCUMENT TRANSFER BETWEEN ELECTRONIC-MAIL NETWORK AND FACSIMILE TERMINALS

Kun Liu, Jan H. Bons and Jens C. Arnbak
Telecommunications and Traffic Control Systems Group
Delft University of Technology, The Netherlands

ABSTRACT This paper presents a system for combining the two present related, but yet separated modes of electronic document transfer, namely, electronic-mail (E-mail) and facsimile. Messages prepared at desk-top terminals, supporting compound document (i.e., text and graphics) creation and editing, and submitted to the E-mail network can thus be received by both interconnected terminals in the common E-mail architecture and by facsimile terminals connected to the public switched telephone networks (PSTN). The latter transmission is achieved by facsimile gateways which connect the two different architectures and perform the necessary protocol conversions.

I. INTRODUCTION

At present, two widely different modes of electronic transfer of documents prove successful: *facsimile* and *electronic mail* (E-mail). The former is based on real-time terminal-to-terminal transmissions between scanning devices attached to the public (circuit) switched telephone networks (PSTN). The latter employs computer networks, providing a message handling service with store-and-forward and multi-addressing facilities. Despite the higher long-distance transmission costs, facsimile appears to be more popular. This popularity is due to the close relation with the familiar paper-oriented correspondence, the ability to handle graphics, the vary large base of well-standardized terminals, and the ubiquitous telephone networks. Electronic mail, on the other hand, has gained support mainly because of the ASCII-oriented corporate communications with features such as personal mailboxes, desk-top editing and document filing facilities [1].

Recently, the feasibility of incorporating graphical features (such as line drawings, maps or charts, signatures, mathematics or music symbols and non-ASCII text) into today's text-oriented E-mail systems was demonstrated, using terminals with writing facilities [2]. The technique, referred to as *telegraphics*[1] permits transfer of *compound documents* (i.e., containing both text and graphics) between interconnected terminals in a common message handling architecture.

The purpose of this paper is to present a system based on the techniques which combine the advantages of the two existing modes of compound document transfer (i.e., telegraphics [2] and facsimile). The system allows generation of compound documents on desk-top PC-based telegraphic terminals, and transmission of these documents both to other terminals in the common E-mail architecture, <u>and</u> to standard facsimile terminals connected to PSTN. The latter transmission is achieved via *facsimile gateways* which connect the two different architectures by performing the necessary protocol conversions. The significance of this system can be projected by the ever growing use of the two services and by the desire to correspond beyond the E-mail architecture [3]. In addition, the former transmission requires only a narrow-band data link, or less transmission time, due to the more efficient coding of texts and line graphics, while facsimile in general produces much larger data size, leading to a requirement of wider bandwidth or more transmission time. Therefore, long-distance document transfer via E-mail and gateways would reduce communication costs, compared with the traditional facsimile transmissions.

II. CODED REPRESENTATIONS OF COMPOUND DOCUMENTS

<u>A. Differential Chain Coding(DCC) of Line Drawings</u>

Line drawings generated by the movements of a stylus on a writing tablet [4] can be encoded based on spatial sampling and vector quantization performed by translating a square coding ring along each curve [2] (Fig.1). A curve l is thus described by the pen-down point p_0, and a vector chain, that is,

$$l = p_0 + \langle v_1, v_2, \ldots \rangle, \qquad v_i \in V,$$

from which l can be reproduced with the pre-defined maximum quantization errors [6],[8]. Here, V is a set of 8M (M = 1, 2, 3, ...) vectors defined by a square coding ring, i.e., $V = \{ \omega_0, \omega_1, \ldots, \omega_{8M-1} \}$, as shown in Fig.1.

---

developed with support from the Dutch Ministry of Science Policy under its telematics program, and from the Dutch PTT.

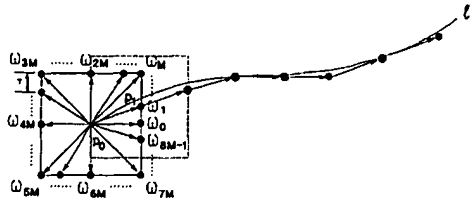
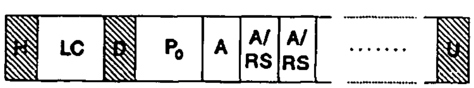


Fig.2 Vector chain coding of line drawings using a square coding ring with 8M sampling points with spacing τ.

In encoding vector chains into binary representation for transmission and storage, data reduction can be achieved by exploiting the statistical dependence between successive vectors. For fluently drawn curves and properly chosen sampling step (determined by $M\tau$), this dependence is demonstrated by a higher frequencies of occurrence of small displacements between successive vectors [7],[8]. Toward this end, Differential Chain Coding (DCC) encodes a vector as a *relative vector* and designates this with a shorter codeword if the displacement (relative to its predecessor) is +1, 0, or, -1. Here, 0 means no direction change, while +1 and -1 indicate one sampling point to the left and right, respectively. Otherwise, the vector is encoded as an *absolute vector* (the first vector of a vector chain is always encoded absolutely). For example, the curve shown in Fig.1 is, in this way, encoded as an absolute/relative vector chain: ω_1, 0, 0, -1, 0, +1, 0. For coding rings with M = 1, 2 and 3, each absolute vector can be encoded as one ASCII byte; each of the three relative vector by 2 bits so that up to 3 successive relative vectors (*vector string*) can be combined to fit into one 7-bit ASCII byte [2].

Fig.2 shows the general construction of the data syntax for DCC encoded line drawings. Data for each curve is packed according to this syntax. The Line Control (LC) contains information such as coding-ring size M, line attributes (color, thickness). LC only appears if it is different from that of the preceding curve; a special code H (header) is used to indicate its presence. The code D (pen-down) indicates the start of data, which is immediately followed by the coordinates of the curve starting point. Then follow the first absolute vector and the encoded sequence of absolute and relative-vector strings. Finally, the code U (pen-up) terminates the data packet.



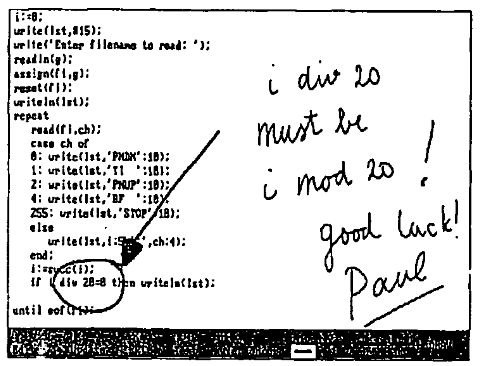
H	Header	(1 byte)
LC	Line Control	(n bytes)
D	pen Down	(1 byte)
P_0	pen-down position	(4 bytes)
A	Absolute vector	(1 byte)
RS	Relative-vector String (3 relative vectors)	(1 byte)
U	pen Up	(1 byte)

Fig.2 Construction of DCC encoded vector chain data packet.

B. Compound Document Representation Format

Based on the above coding technique, a compound document page with text and line graphics is represented by ASCII bytes, and appears to message handling network in the format of pure ASCII strings. Receiving telegraphic terminals must decode it to restore the text and graphics on screen or in the form of hard copies.

An E-mail document page thus consists of two blocks of ASCII codes representing, respectively, text and line graphics on the page. We chose to identify the text block by an unique character combination "!h" in front of the block. The separation of the graphics block from the text block is achieved by heading each graphic ASCII line with "!g". Obviously, message lengths are variable. In Fig.3, an example is shown, where (a) is the screen dump of a message consisting of both text and line graphics, and (b) is the print-out of the message codes. The total data size of this compound page is 1,434 bytes.



(a)

```
!h15
i:=0;
write(lst,#15);
write('Enter filename to read: ');
readln(g);
assign(fi,g);
reset(fi);
writeln(lst);
repeat
   read(fi,ch);
   case ch of
   0: write(lst,'PNDN':10);
   1: write(lst,'TI  ':10);
   2: write(lst,'PNUP':10);
   4: write(lst,'BF  ':10);
   255: write(lst,'STOP':10);
   else
      write(lst,i:5,':',ch:4);
   end;
   i:=succ(i);
   if i div 20=0 then writeln(lst);

until eof(fi);
!gl(DBBOP)Q^LjyPB)C21(DBAOQGRY21(DBBOSRQ]E)Gl)KeN}PBgr^}LjsnOA
!gghEMc-BD^)N^PBD^yIKOA{21(DBAOTIRj21(DBBOVdREF}B}N)Lj_)E)Aeg)
!gDrMogCyF|H|JL2OPNNmMnssEs\q)OMnssEsaq}MsruPCpc}LjwOCes-Ljp-A
!g-D^s-Om)L)J)E[jsnyMnnc}Pg-20SIOMAsd-20UKNRBgsp)GILN'nj)A-Dr-
!gNPirxIKMp{Ap20PnJyLj{PjgE20P{KtP20RtKUMss)DruCyBNms|Ele}AMp|
!gAfq-L)Mr-AD}Er)PeclHJgyOACjnj-Mr\j-B-20WTLFD-CtN)Ldq-E}B{p-D
!g}E|MpPo)DyGo]}K20[_OBN2lmc'^u20ZuKFByIf-PBFH21(IBBOT(HEE)GIr
!gyMr-AojyLjsnsramJGa_qhlq{HLwN^PBDoxPjc)Kg)PxD{HB'\IKg)AfshF'
!gMsr`gi)20YZIGE)Mlsr|Po)Ds|LpyPCi)MOvP-C-20[gH\HyKMifD20\LIjM
!gnss]E[zJg-OA{20]FJCNas^)21(IBAO]IGm21(IBBOVPEkMsssslranF\)20
!gUxE[D)Bmm-Oc[Lm'Ih)20XSDmDF-If}M^-PBphEvLo}Ofi^nLj|OACjd-MwO
!gfni}'|HJor^r)Ppy20WHBEAjsqhj^ls^lqj^^lll121(DCAOGnFU21(DCCOG
!gcFfOD]a^ladslll\js^z20GlGBRnyGsswS's)CsvMe-Bn|ILn)WjNLyWyKMK
!g}ShwH)QSGSEwGLPB}DFSuF)H-EA)W}KpyAavUP\|FC{NFHyKCXlzRLGM\)21
!g(DCAOHOIP20GXEtDj^l^lsqjsssssnqiassdsdnr\nczGandjsnc-GjqAac
!g\c^^^^ls^sssqiassdrac\p^sncl^l{Ber\cnnnwF2
```

(b)

Fig.3 An example of compound telegraphic document page. (a) screen dump. (b) message codes in telegraphic format.

III. Structure of E-mail to Facsimile Conversion System

Facsimile gateway are used to connect the two different network architectures by performing the necessary protocol conversions. Fig.4 illustrates a model for this conversion. The essential part is the transcoding which converts an E-mail message into the CCITT standard facsimile message format.

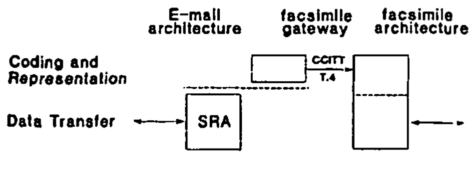
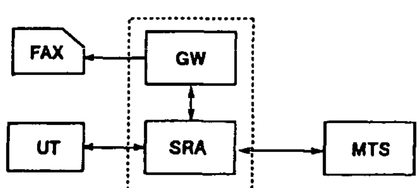


Fig.4 A model of protocol conversions between E-mail and facsimile.

One of the design considerations for the system structure is that message conversions should take place closely to destination facsimile terminals. This is because of the increase of data size of generally 10-20 times when converting an E-mail message into the CCITT standard facsimile data format. A physical mapping of a gateway within the E-mail system is shown in Fig.5. Here, MTS (Message Transfer System) and SRA (Submission/ Reception Agent) are the entities of the E-mail system. MTS provides application-independent data transfer. SRA interacts, on one hand, with MTS in order to submit messages to or receive messages from it and, on the other hand, with user terminals in order to transfer messages via the mailboxes in which messages received from MTS and messages for submission to MTS are (temporarily) stored.

In Fig.5, the gateway (GW) and SRA are co-resident in the same processing system. Any incoming messages intended for local facsimile terminals are relayed by SRA to the gateway for processing and delivery. The information relayed includes a relay-envelop, in addition to message contents. Among other items (such as sender's identifications, message identifications, service requests, etc.), destination facsimile terminals are specified in the relay-envelop, which are provided by a sender when submitting the message.



FAX facsimile UT E-mail User Terminal

Fig.5. A facsimile gateway within a standard E-mail network.

IV. Description of Facsimile Gateways

A. Service Elements

The gateway software should support at least the following basic service elements: message conversions, facsimile communications and failed-delivery notifications.

(a) Message Conversion: An E-mail message intended for facsimile terminals is received by SRA and relayed to a facsimile gateway for processing. The gateway converts the E-mail message into the format suitable for reception by facsimile terminals.

(b) Facsimile Communications: A facsimile message is sent to one or more destination facsimile terminals specified by the sender, using the standard communication procedures recommended by CCITT [9].

(c) Failed-delivery Notification: An attempt to deliver a facsimile message may fail for various reasons (invalid facsimile number, terminal engagement, incompatibility, or defects of equipment). Depending on the type of failure, redial of the destinations may be invoked automatically after a defined time interval. The final failure will cause the delivery to be aborted, and a failed-delivery notification (FDN) is provided. The FDN message is delivered to sender's mailbox by E-mail.

B. Message Conversion Algorithm

An E-mail message is ASCII-encoded and may consist of both text and line graphics. The corresponding facsimile message is obtained by pixel-based encoding of the overlay of text and graphics. To convert an E-mail message, the facsimile gateway maintains a two-dimensional bit-array which has numbers of rows and columns corresponding to the facsimile resolutions. For standard Group 3 facsimile [9], this array has 1728 columns and 1076 rows. A bit in the array is '1', corresponding to a black pixel, or '0', to a white pixel. The process of conversion includes three steps and involves a fair amount of computation and bit manipulation.

The first step is to convert each line of text characters into a two-dimensional matrix of pixels and then place them into the appropriate position in the bit-array. The pixels for each character are taken from a look-up table containing the character font specified.

The second step is to overlay line graphics onto the bit-array. This involves a decoding process of vector chains. Each vector (absolute or relative), is a straight line segment and can be mapped onto the bit-array using a line algorithm. For each chain, the starting point of one vector is the ending point of the previous vector, except the starting point of the first vector. This is the pen-down point given in the vector chain data packet (Fig.2).

And finally, at the third step, each row of bits in the bit-array is encoded using the standard facsimile coding scheme [9]. The coded data is buffered in a binary file, ready for transmission to the destination facsimile terminals.

V. Evaluations of E-mail — Facsimile System

In this section, we present an extensive comparison of the two present modes of compound document transfer: telegraphic and facsimile. The integration of the two systems based on the use of facsimile gateways combines most of the advantages of the both modes.

In general, facsimile is based on real-time terminal-to-terminal transmission of (pre-prepared) paper-oriented documents via PSTN. The major advantages of it are:

- internationally standardized, ensuring world-wide interworking of terminals from different manufacturers, via PSTN, the most widely available network throughout the world;
- a large (and still growing) installed base of facsimile terminals, which allow flexible exchanges of documents;
- the ability to exchange compound documents (i.e., text and graphics);
- low local transmission costs within most national PSTNs, due to the relative modest telephone tariffs for local calls.

Against this, however, there are at present also a few significant disadvantages of facsimile:

- no desktop editing and document filing facilities;
- at most copy quality of document transfer;
- large data size (e.g., by Group 3 facsimile coding, generally well above 25 kilobytes per page);
- the high long-distance transmission costs of international telephone traffic apply.

Most of these shortcomings, however, can be avoided in the telegraphic system, which also provides additional advantages:

- integration into multi-functional individualized computer-based workstations allowing desktop editing, transmission and receiving, and filing of documents;
- first-level printout quality of documents at receiving ends;
- much smaller data file sizes, due to the efficient ASCII coding of text and line graphics.
- lower long-distance transmission cost compared to facsimile;
- security is provided by the network architecture, e.g., personal mailboxes, passwords.
- ready adaption to different networks (public or private, circuit or packet switching) in order to reduce transmission costs or to achieve point-to-multipoint connectivity.

The transmission costs are of particular interest to many system users. For terminal-to-terminal document facsimile transfer, the costs are proportional to the data sizes. In Fig.6, a cost comparison is shown for document transfer by facsimile and telegraphic. This comparison is based on transmitting documents from the Netherlands to four destinations, namely, domestic (within the Netherlands), another European country, the US, and Japan. We assume an average data size is 25 kilobytes for a facsimile page, and use a data reduction factor of 15 to derive the telegraphic data file size. The present structure of domestic telephone tariffs is seen to favor the local use of facsimile. However, international transmissions are always cheaper by E-mail, except for single-page transmission (1 page) to another European country. The cost reduction possible for international transmission of documents using E-mail and local facsimile gateways is considerable.

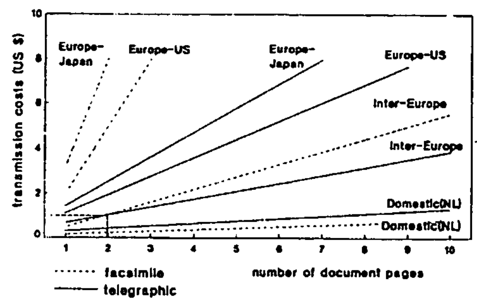


Fig. 6 Comparison of facsimile and E-mail document transmission costs by public networks, from The Netherlands to another terminal in (i) The Netherlands (NL), (ii) the United Kingdom (Europe), (iii) the United States (US), and (iv) Japan. (tariffs as of April 1, 1988).

VI. Conclusions

In this paper, a system for electronic transfer of documents is presented, that allows compound document interchange between E-mail and facsimile through facsimile gateways embedded in the E-mail architecture. The significance of this integration can be projected from the growing use of the two related, but separated services. A extensive comparison of the two modes of document transfer is performed. Major cost reductions in long distance document transfer is possible with respect to the traditional facsimile communications via the PSTN. This is brought about by the efficient DCC graphics encoding, and the present tariff structure of international telecommunications.

Acknowledgement The authors are like to thank Professor R. Prasad for his valuable suggestions.

REFERENCES

[1] Peter H.M. Vervest, "Electronic-mail and message handling", Francis Printer, London, 1985.

REFERENCES

[1] Peter H.M. Vervest, "Electronic-mail and message handling", Francis Printer, London, 1985.

[2] J.C. Arnbak, J.H. Bons and J.W. Vieveen, "Graphical correspondence in electronic-mail networks using personal computers", IEEE J. Selected Areas in Comm. Vol. SAC-7, pp.257-267, Feb. 1989

[3] J.C. Arnbak, "Transborder communications networks: technology driven or social innovation?", European Management Journal, Vol.6, No.4, November, 1988.

[4] L.R. Nieuwkerk, "A writing tablet for converting handwritings into electrical signals", NERG Tijdschrift, Vol. 38, No.6, 1973.

[5] D.L. Neuhoff and K.G. Castor, "A rate and distortion analysis of chain codes for line drawings", IEEE Transactions on Information Theory, Vol. IT-31, No.1, pp. 53-68, Jan. 1985,

[6] K. Liu and R. Prasad, "On the quantization distortions and coding efficiency of line-drawing graphics transmissions using Differential Chain Coding", Proceeding ICC'90, Atlanta, USA, pp. 325A.2.1-325A.2.5, April, 1990.

[7] A. Kegel and J.H. Bons, "The coding of dynamographical information with application to Scribophone, Teleboard and Vidiboard", in New Systems and Services in Telecommunications, Vol.2, North-Holland, 1984, pp. 439-445.

[8] R. Prasad, J.C. Arnbak, J.W. Vieveen and J.H. Bons, "Relative vector probabilities of line drawings using Differential Chain Coding", in Proceeding IEEE Pacific Rim Conference on Communication, Computer and Signal Processing, Victoria, B.C., Canada, pp. 138-142, June, 1989.

[9] CCITT Recommendation, T-series, "Terminal Equipment and Protocols for Telematics Services", Geneva, 1989.

Compound document transfer between electronic-mail ne facsimile terminals

Liu, K. Bons, J.H. Arnbak, J.C.
Delft Univ. of Technol., Netherlands ;

This paper appears in: **TENCON 90. 1990 IEEE Region 10 Conference on Computer a Systems**
Publication Date: 24-27 Sept. 1990
On page(s): 644 - 648 vol.2
Meeting Date: 09/24/1990 - 09/27/1990
INSPEC Accession Number:4045128
Digital Object Identifier: 10.1109/TENCON.1990.152689
Posted online: 2002-08-06 17:19:26.0

Abstract
The authors present a system for combining the two related yet separated modes of elec transfer, namely, **electronic-mail** (E-mail) and facsimile. Messages prepared at desk-top compound document creation and editing, and submitted to the E-mail network can thus interconnected terminals in the common E-mail architecture and by facsimile terminals c switched telephone networks (PSTN). The latter transmission is achieved by facsimile ga the two different architectures and perform the necessary protocol conversions

Index Terms
Inspec
Controlled Indexing
electronic mail electronic messaging facsimile

Non-controlled Indexing
E-mail PSTN compound document creation electronic document transfer **el** network facsimile gateways facsimile terminals graphics protocol conversio switched telephone networks text

Author Keywords
Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEE Xplore.

Securing electronic mail systems

Serenelli, B. Leisher, T.
USA CECOM, Ft. Monmouth, NJ, USA;

This paper appears in: **Military Communications Conference, 1992. MILCOM '92, Cor 'Communications - Fusing Command, Control and Intelligence'., IEEE**
Publication Date: 11-14 Oct. 1992
On page(s): 677 - 680 vol.2
Meeting Date: 10/11/1992 - 10/14/1992
Location: San Diego, CA
INSPEC Accession Number:4471286
Digital Object Identifier: 10.1109/MILCOM.1992.244144
Posted online: 2002-08-06 18:21:39.0

Abstract
It is pointed out that security at the network layer cannot provide application-specific serv **electronic mail** such as signed receipts and digital signatures. These deficiencies can b providing end user to end user security where mail messages are black (protected/encry intermediate points. The authors describe the approach and implementation taken in buil security device. Mail messages are protected along the entire path from originator to reci are protected during storage and processing at all intermediate points. the security can b independently of the network layer architecture or a network layer security device. The ke technique is suitable for client-server architectures such as **electronic mail**, where the n large and connectivity is diverse

Index Terms
Inspec
Controlled Indexing
computer networks cryptography **electronic mail**

Non-controlled Indexing
client-server architectures digital signatures **electronic mail systems** messa encryption message protection network layer security signed receipts
Author Keywords
Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEE Xplore.

SECURING ELECTRONIC MAIL SYSTEMS

BOB SERENELLI TIM LEISHER
USA CECOM, C^3 Systems Directorate
Information Security Division, Ft. Monmouth, NJ 07703

Abstract:

Securing electronic mail presents some unique challenges in that it is a staged delivery application, where the message originator and message recipient are not usually in real-time communications with each other. For applications such as electronic mail, network level encryption devices leave vulnerabilities at intermediate relay points such as mail servers or message transfer agents (MTAs).

Mail messages are typically decrypted, and stored RED (unprotected/unencrypted) at these repositories. Subsequently, they are re-encrypted and delivered to their destinations (see fig 1).

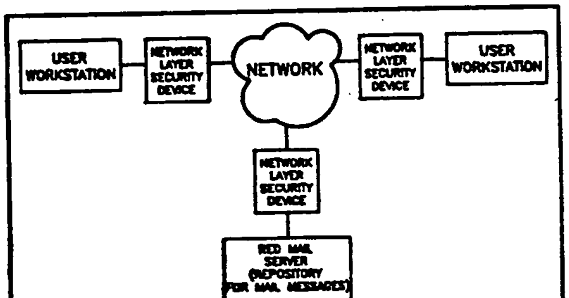


Fig. 1 Network Mail System

Security at the network layer can not provide application specific services associated with electronic mail such as signed receipts and digital signatures. These deficiencies can be remedied by providing end user to end user security where mail messages are black (protected/encrypted) at all intermediate points. This paper describes the approach and implementation taken in building such a mail security device. It shall address the key security services provided and possible implementations.

Approach:

The staged delivery (non-real time) nature of E-Mail levies the requirement that each security device must execute security relevant process/decisions (i.e., confidentiality, integrity, source authentication, access control) without a real-time exchange of information between cooperating parties. The large base of electronic mail users and their diverse connectivity requirements make the use of secret keys distributed from a trusted source impractical and undesirable. The mail protocol will use a staged key information exchange in which a user to receive secure mail posts his certificate and some public key information on a mail or directory server. The sender uses this posted information along with his own private information to process a pair-wise key encryption key, which is unique to the sender-receiver pair.

The protocol accommodates multi-addressing by using a single message key to encrypt the message and then using a pair-wise key, for each addressee, to encrypt the message key. The message header includes the sender's certificate. It also includes for each addressee, the public key information needed to process their pair-wise key, the encrypted key and the integrity check.

The electronic mail security device performs the following security functions.

ENCRYPT MESSAGE
OUTPUT CREDENTIALS
HASH MESSAGE
GENERATE SIGNATURE
READ CREDENTIALS
GENERATE KEYS
ENCRYPT KEYS
DECRYPT KEYS
DECRYPT MESSAGE
READ SIGNATURE

Credentials refer to a users certificate and public key information to include keying information needed for the generation of digital signatures.

System Operations:

The transmission of a secure electronic mail message involves a sequence of steps as shown in Table I. Each user has unique keying information which is bound to a non-forgeable certificate. The certificate identifies the end user and their security privileges. Two users wishing to communicate exchange certificates and keying information. The exchange results in a key that is pair-wise unique between the two end users. Establishing a pair-wise key requires the principles to gather each other's public information. This information can be obtained from a mail/directory server much in the same manner that phone numbers are taken from telephone books. The certificate is digitally signed by a certifying authority that all members trust. This eliminates the need for trust at the servers since certificates can neither be forged or altered. Certificates may also be cashed by end users to eliminate needless requests to the server.

The mail message format is shown in Figure 2.

Privacy of the message is achieved because only the correct recipient possesses the pair-wise key and can decrypt the message (steps 4,5,6,7,11,12,13). The source of the message is authenticated by the binding between the sender/receiver credentials and the pair-wise key (steps 1,2,3,10). The source of the message can

TABLE I - SECURE MAIL TRANSFER

SENDER	RECEIVER
	1. Transmit Recipients Credentials
2. Receive Credentials of Recipients	
3. Transmit Credentials of Sender	
4. Process Key (Key Encryption Key)	
5. Generate Key (Traffic Encryption Key)	
6. Encrypt Key (Encrypt TEK with KEK)	
7. Encrypt Message with TEK	
8. Hash Message	
9. Generate Signature	
	10. Receive Senders Credentials
	11. Process Key (KEK)
	12. Decrypt Key (TEK)
	13. Decrypt Message with TEK
	14. Read Signature
	15. Hash Message
	16. Generate Signature
17. Read Signature	

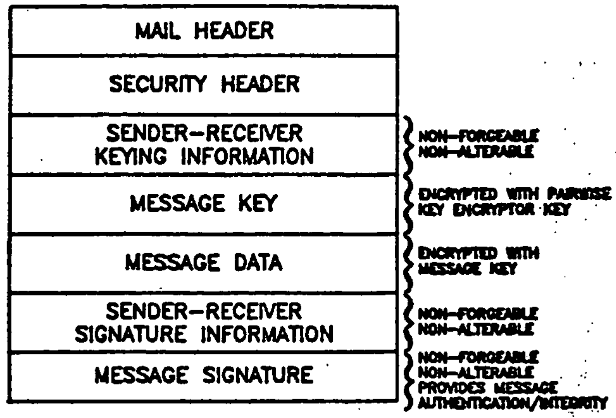


Fig. 2 Voice Message Format

also be authenticated by the sender cryptographically signing the mail message. This can be useful if authentication without privacy is desired (steps 8,9,14,15). Authentication of end users identity is achieved through the exchange of non-forgeable certificates (steps 1,2,3,10). Integrity of the message is maintained through use of a digital signature appended to the message. Insertion, deletion or modification to the mail message results in an invalid signature at the receiver (steps 8,9,14,15). The mail transfer scenario

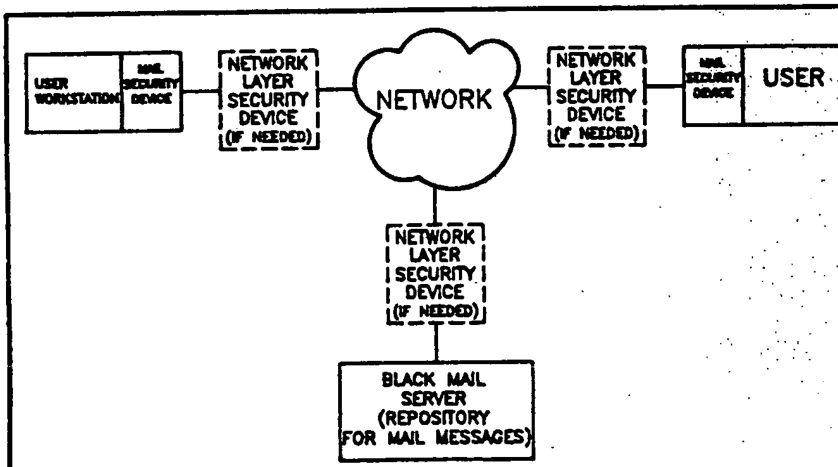


Fig. 3 Network Layer Security Devices

provides the capability of sending registered mail. The sender can not deny having sent mail since the sender is the only party to have his unique signature key (proof of origin) (steps 8,9). The receiver provides proof of delivery by resigning the hashword on the message with his unique signature key and sending the resigned hashword back to the sender (steps 15,16).

If link, network or transport layer security services are employed, they will act independently of the application layer security services discussed in this paper. The new architecture that arises from using the secure E-Mail device is shown in Figure

3. A network layer security device may be used to protect mail header information or to secure other types of data traffic not secured by the mail security device.

Summary: This paper described an approach at protecting mail messages along the entire path from originator to recipient. The messages are protected during storage and processing at all intermediate points. The security can be implemented independent of the network layer architecture or a network layer security device. The key distribution technique is suitable for client-server architectures such as E-mail where the number of users is large and connectivity is diverse.

You requested this document:

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. **CAFE: a conceptual model for managing information in electronic mail**

Takkinen, J.; Shahmehri, N.;

System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conferen
Volume 5, 6-9 Jan. 1998 Page(s):44 - 53 vol.5

Abstract:

The design and implementation of a conceptual model, CAFE (Categorization Assistan
described. The model supports the organization, searching and retrieval of information
modes are available for satisfying the users' needs in various situations: the busy mode
use at times of high stress; the cool mode for continuous use at the computer; and the
sporadic use when exploring and (re-)organizing messages when more time is at hand
the model is motivated partly by the results of a case study of categorization on the cor
and partly by a survey of e-mail clients. The case study was inspired by cognitive scien
model is related to information seeking theories in electronic environments. In the imple
mode required using a different technique. The busy mode uses the text-based Naive I
algorithm, the cool mode uses e-mail filtering rules, and the curious mode uses a comb
clustering techniques known as scatter/gather

Abstract | Full Text: PDF(1272 KB) **IEEE CNF**

CAFE: A Conceptual Model for Managing Information in Electronic Mail

Juha Takkinen and Nahid Shahmehri
Laboratory for Intelligent Information Systems (IISLAB),
Department of Computer and Information Science, Linköping University, Sweden
`juhta@ida.liu.se` and `nsh@ida.liu.se`

Abstract

The design and implementation of a conceptual model, CAFE (a Categorization Assistant For E-mail), is described. The model supports the organization, searching, and retrieval of information in e-mail. Three modes are available for satisfying the users' needs in various situations: the Busy mode for intermittent use at times of high stress, the Cool mode for continuous use at the computer, and the Curious mode for sporadic use when exploring and (re-)organizing messages when more time is at hand. The design of the model is motivated partly by the results of a case study of categorization on the computer screen, and partly by a survey of e-mail clients. The case study was inspired by cognitive science theories. The model is related to information seeking theories in electronic environments. In the implementation each mode required using a different technique. The Busy mode uses the text-based Naive Bayesian algorithm, the Cool mode uses e-mail filtering rules, and the Curious mode uses a combination of clustering techniques known as Scatter/Gather.

1. Introduction

Electronic mail (e-mail) is the preferred communication medium for an increasingly growing number of users around the world. It is one of the "killer applications" of the network world today. Moreover, e-mail affects social factors and patterns of communication within an organization [28].

E-mail is used both at home and at work and important e-mail messages are increasingly often being mixed with less important messages in the evergrowing flow of information between users. Increasingly often users find it difficult to search and retrieve information in e-mail messages. Furthermore, people tend to collect and store information for later use, for personal business and, typically, for supporting decision-making [22]. In e-mail and computer conferencing systems, such as KOM [20] and netnews (Usenet News), the storing of information is easy, while the retrieval of it often is more difficult. Moreover, it is easy to quickly disseminate information to many recipients at the same time. This *asymmetry* is characteristic of the electronic messaging systems being used today. As Marchionini [16] (p. 1) states, the general consequences of the information society we live in are threefold: we have larger volumes of information, new forms and aggregations of information, and new tools for working with information. Furthermore, we also have more complicated information needs [9].

The e-mail user is rapidly finding herself in dire need of some kind of help in *structuring* and getting a better *overview* of the information contained in her e-mail messages. Furthermore, she is in need of retrieving the information in better ways. The amount of effort required to retrieve relevant information is related to the amount of information stored. Among the major reasons for the information retrieval difficulty are the lack of explicit semantic clustering of (or linkages between) relevant information and the limits of conventional search techniques using keywords (either full text or index-based) [39]. Especially, the organization of incoming messages becomes more critical as the amount of e-mail messages in the system grows. A system with support for classifying the information would help the recipient in her task of reading and selecting relevant messages and avoiding "junk mail" or other messages of low interest. Moreover, the support for the management of the information contained in e-mail messages has to consider both the static storage of messages and the dynamic flow of incoming messages. Finally, to make it possible for the user to satisfy her information needs, the system must allow the user to search for messages by entering queries—and examine the retrieved messages—interactively, and with a response time of only a couple of seconds.

In this paper we describe a conceptual model for the information management in e-mail. We look for inspiration in two places: cognitive science theories for categorization, and available techniques for retrieving and displaying e-mail messages, and organizing them on the computer screen. We concentrate our efforts mainly on textual information because e-mail is (still) a mostly textual medium. In section 2, we start by first looking at categorization, which is the basic principle behind information management. In section 2.2, the conclusions from a case study of people's categorization of e-mail messages on the computer screen are presented. The

1060-3425/98 $10.00 (c) 1998 IEEE

findings from a survey of the filtering, organization, and visualization capabilities of some currently available clients are summarized in section 2.3. Based on conclusions from the case study and the survey, we then construct our conceptual model CAFE in section 3 and present a prototype implementing the model in section 4. We conclude our work and give some directions for future work in sections 5 and 6, respectively.

2. Background

2.1 Cognitive science theories for information categorization

Categorization of information is studied in both cognitive science and information retrieval and filtering (IRIF). According to psychologists there are two general and basic principles for creating categories: *cognitive economy* and *perceived world structure* [25]. These principles state that the function of categories is to provide maximum information with the least cognitive effort, and the attributes, or features, that an individual will perceive in the world, and thus use for categorization of stimuli, are determined by the needs of the individuals. Moreover, these needs change over time and with the physical and social environment. The maximum information with least cognitive effort is achieved if categories map the perceived world structure as closely as possible [25]. Since the perceived world is different for each individual, the categories are indeed personal to the individuals using them. *Similarity* plays a central role in placing different items into a single category. The similarity of the items in a category varies, but to a certain degree—people want to minimize within-category variability of similarities between items while maximizing between-category variability [27]. However, similarity is really "in the eye of the beholder" and does not alone explain categorization, since no constraints are provided on what is to count as a feature or attribute [32].

Categories and personal knowledge structures are of central interest to cognitive psychology researchers. The cognitive psychologists' models of categorization and the human memory can provide useful clues for making the retrieval of information easier and more intuitive [33] (p. 178). Through the history, different theories for how categories are structured and created by humans have evolved [7]. Three examples are *the classical view, the probabilistic view*, and *the theory-dependent view.*

The first two define categories solely based on the features or attributes that the items put in the categories have [25][32]. Of these, the classical view, first presented by Plato, describes categories as structured around features that define all of the items in each category. The probabilistic view, on the other hand, describes categories as either organized around a prototype or best example, or represented by all the individual instances that constitute it. The first variant of the probabilistic view is called the prototype view and the second variant is called the exemplar view.

In the theory-dependent view categories are based on knowledge and world theories (theories that humans use in categorization tasks). In other words, people's individual theories determine the features that will be important for a category.

The research on categorization in cognitive science has progressed from the classical to the probabilistic view and from the idea that concepts are organized around similarity to the idea that concepts are organized around theories (Medin 1989, in [32]).

Two examples of using the above mentioned theories for categorization in the IRIF area are neural networks (for example, [17]) and fuzzy sets [24]—the latter is, by the way, an attempt to use Rosch's prototype view [25] for modelling categories. Inspired by the cognitive theories, we designed a case study to learn more about the physical and mental processes of people when they sort messages on the computer screen.

2.2 A case study of categorization on the computer screen

The purpose of the case study was to examine how people create structures on the computer screen and how the structures evolve when increasingly more messages are sorted into them. A special structure editor was developed for the case study (fig. 1; [12]). Twelve users of e-mail acted as subjects. Each subject was asked to sort a number of previously unseen e-mail messages into categories of their own devising. Five types of queries were used to test the efficiency of category structures for retrieval, ranging from simple keyword-based queries ("What messages contain the URL http://www...?") to situation-based queries ("What messages contain relevant information if you are a music teacher and you want to start exploring music resources on the web?"). Among other things, the number of relevant hits was counted and the retrieval time was measured. Also, we wanted to see how different representations of categories influence the development of structures and the retrieval of messages. We used three different representations of the messages and the categories on the computer screen were used: *the desktop metaphor* (cf. the Macintosh environment), *the tree structure* (cf. the file manager in Windows 95), and *the mind map* [2]. The mind map (fig. 1) is a two-dimensional, hierarchical structure that provides the subjects with different layout functions, such as line thickness and red lines for links between categories [12], for organizing messages and categories. Furthermore, we wished to examine what

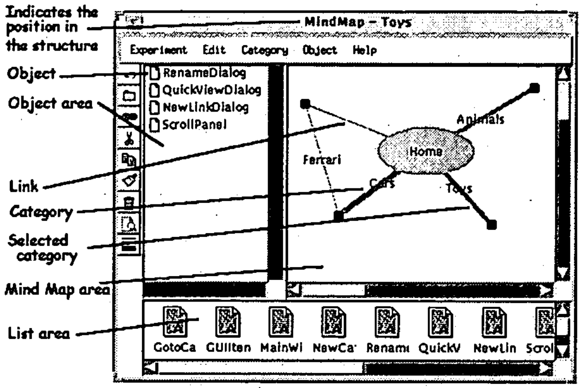


Figure 1. An example of a mind map as displayed in the structure editor used in the case study.

happens with the structures when messages with contents that differ from the main contents of the other messages ("junk mail") are presented to people and how these messages are sorted into the structures. For this purpose, two different mailing lists were used: one with messages relevant to the subjects' background (about choir singing [41]) and another one with supposedly irrelevant messages. Finally, we hoped to learn more about what different features of the messages people use in the categorization procedure—the categories of each subject were regularly measured for their within-category and between-category variabilities and the criteria used for grouping messages were determined.

The case study was a continuation and expansion of a previous preliminary study of people's categorization of text (e-mail messages and proverbs) on pieces of paper on a table [3][23][30]. For details about the set-up for the case study, see [31].

The categories created by the subjects were not perfect—many subjects stated that they were not satisfied with the structures they had created. However, the results do give some hints for some usable information management and categorization principles.

The desktop was the most familiar structure to the subjects. However, it was very cumbersome to use and offered a poor overview of the collection of messages. The subjects in the desktop group clearly wanted some other means of navigating and grouping messages in the structure.

The hierarchical tree structure was the most efficient one for retrieving messages. The subjects were able to easily browse the categories in an orderly fashion. This was awkward and time-consuming to do in the desktop structure, and even more so in the mind map structure. The tree structure was very familiar to most of the subjects, although the structure became cluttered when increasingly more categories were created.

The mind map was the least familiar representation of the three used. The two-dimensional format of the mind map seems to have had, at the same time, a stimulating and a constraining effect on the sorting procedure. The main advantage with the mind map was that the whole organization of message categories was visible and available at the same time. Furthermore, it could be highly personalized in a spatial and graphical way, where related items and categories were clustered via spatial proximity.

The number of categories was in the mind map group the smallest in mean, but at the same time the range was the largest. Furthermore, the subjects in the mind map group seemed to form more associations with matching messages than the subjects of the other groups did to locate messages. The *Subject* line of the messages was extensively used for naming the categories, which is a result similar to an investigation made by the IntFilter Project at Stockholm University [11] (p. 26). The subjects were heavily reorganizing their structure for the categorization of the "junk mail" that was presented to the subjects. The *type* of messages influenced more the number of categories than the *number* of messages. Finally, there seems to be a need for a flexible way of changing the view of categories (folders), depending on the task (searching, sorting, etc.) that is to be performed. For a more detailed description of the results and analysis of the case study, see [31].

2.3 State-of-the-art of information management in e-mail clients

Studies have shown a wide level of diversity in the way people use their e-mail clients and also a wide range of tasks for which they are used [14][29]. One problem with e-mail systems is that the e-mail client often is only a thin layer on top of the delivery system [8]. In a survey of e-mail clients available for Internet-style e-mail (e-mail using SMTP and POP3/IMAP protocols) we investigated what different functions were available for the organization of messages and visualization of collections of messages [31]. The survey revealed a great uniformity of available functions. Filtering functions for handling incoming messages are common, as are the use of folders for storing messages and two-paned or three-paned displays (fig. 3 in section 4) for presenting messages on the screen.

The most basic information management offered to the user in the e-mail client consists of the following functions: incoming messages are put (automatically by the delivery system) in an *inbox* and, typically, outgoing messages into an *outbox*, the user can read, print, compose, and send messages, and she can create folders (mailboxes) and manually file messages into the folders for permanent storage.

The folders can be created according to an organization principle of the user's own devising and often in a

hierarchy. Usually, messages can be sorted into folders by way of a drag-and-drop interface that lets the user move around messages among folders with greater ease. Other functions or features commonly available in the e-mail client are the following:

- there is a folder list, a message summary, and a one-message preview window
- the filtering system looks at the text in the *From* and *Subject* lines of a message and, depending on the filter rules, moves messages into folders
- the messages can be searched for words
- the messages can be addressed through the use of aliases and addresses can be stored in an address book.

Most up-to-date clients offer a whole system of filters or rules that the user can use for automatically performing actions on (route, print, and otherwise process) incoming messages. *BeyondMail* [35] is one example and *Exmh* [36] another, each representing different approaches. BeyondMail is a commercial product. It is part of an integrated environment called groupware, which also includes bulletin boards, group schedules, and document flow, but also available as a standalone application with a lot of usable functions for organization of e-mail. Exmh, on the other hand, is a freely available and highly customizable program, with a multitude of user-definable functions for filtering, organization, and getting an overview of e-mail. Some clients even provide programming tools—powerful scripting languages—that can be used to build applications or trigger elaborate processes based on incoming e-mail [35][42]. Many times, however, these tools are hard to use, even at a basic level, e.g., Ishmail's patterns for rules [40]. Finally, the search functions vary from simple searching of words in message headers in one folder to advanced Boolean searching in all folders at the same time—cf. Exmh [36].

Most commonly, the vendors of the commercially available e-mail clients in our survey make the assumption that both sender and recipient of e-mail use the same product, i.e., the vendor's product. This makes it of course easier to incorporate handling of, e.g., *priorities* of messages (Urgent, Regular, etc.) and *forms* for special types of messages (meeting, phone message, etc.)—cf. BeyondMail [35]. These vendor-specific features can be of valuable use when creating a personalized structure of message categories. They can make the structure more meaningful and flexible to the individual user. Furthermore, sorting the received messages into categories according to priority coding or type of message helps making the messages more retrievable and viewable in new ways. However, few e-mail clients fully support this functionality without relying on vendor-specific features.

3. CAFE: The conceptual model

How much of the work of classification of a message can be put on the sender and the recipient of the message respectively? We argue that the asymmetry in e-mail (see section 1) is both necessary and unavoidable. The sender does not want to manually classify a message, since it would mean more work. One solution could be to introduce a common collection of categories for e-mail users and their messages. Using this classification system, software could be used to automatically classify messages before sending them. However, this would mean that each and every e-mail user should have the same kind of software for classifying and recognizing messages. Furthermore, the classification system would most certainly be difficult to maintain. Managing the software would be practically impossible, considering the wide variety of e-mail clients available [31]. Also, the classification system can be misused, e.g., classifying messages as being of high priority when they are not [28] (p. 75). The burden of categorization of messages should be put on the recipient's side instead. Hence, our aim is to aid the recipient in the classification, organization, and getting an overview of her set of messages.

Furthermore, putting the solution in one "monolithic" package, i.e., using one technique to take care of all cases of message handling, is not what we want to do. We want to make it possible for the recipient of messages to use different methods when looking at the information in her e-mail. The current state of mind of the recipient is important. For example, does she have little or much time to spend on reading messages and what is the information she needs at the moment? Therefore, we want to make is possible for the user to explicitly tell the e-mail client what her current state is.

According to the principle of perceived world structure (see section 2), a computerized system for text categorization should be flexible in its management of the text and its representation of the user. By this we mean that text should be possible to classify in different ways, according to the needs of the user. This flexibility requires domain knowledge that changes over time. The knowledge about texts and users is usually modelled as a combination of the document representation and the (explicitly or implicitly defined) profiles of the user in the system. An example of a categorization system with these features is given by [13].

Our conceptual model for a Categorization Assistant For E-mail (CAFE) makes use of three different modes for specifying the user's state. Through the different modes, CAFE is designed to support different strategies for reading, sorting, and searching messages. Both analytical and browsing strategies are supported. Generally speaking, these strategies are central for overcoming the information

problem [16] (pp. 7–8) and alleviating the user's "anomalous state of knowledge" (ASK) [1]. The conceptual model is shown in fig. 2. The modes are:

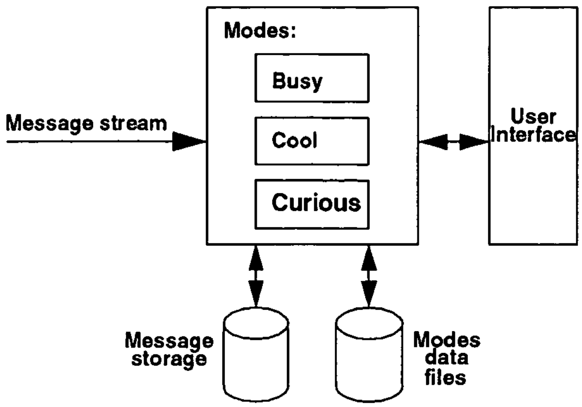


Figure 2. The conceptual model CAFE.

- The *Busy* mode is designed to be used *intermittently*, for locating important messages among the latest messages in the message storage. The user is typically in a situation when she has little time for reading new and unseen messages. The user is presented with a prioritized list of messages, grouped into the categories (folders) *Important*, *2nd Class*, and *Junk* [6].
- The *Cool* mode is the default mode designed to be used *continuously*. It operates on the incoming message stream. The Cool mode is used in situations when the user can read messages little by little during her session at the computer. The user's own categories are used for storing the messages.
- The *Curious* mode is designed to be used *sporadically* (typically once a day), in situations when the user has time to spare. The mode is employed when the user wants to locate, organize, or reorganize previously stored messages. It supports the analysis of a larger collection of messages, typically messages from a mailing list, in all or a subset of the folders in the message storage. The user is presented with groupings of messages where she interactively can select categories to "zoom in on" and investigate further.

The main guiding principle in the design of the conceptual model of CAFE has been to let it contain alternative representations. The user is allowed to select from the three representations (modes) according to her current personal style, experience, and information problem. This approach with using alternative representations is argued for by [16] (p. 140). The main argument is that cognitive science offers a variety of theories about how humans categorize and represent information and knowledge (see section 2.1). The need for flexibility in the representation of categories was also implied by the results of our case study of categorization in e-mail (see section 2.2). Moreover, the use and usage of e-mail in general [14] have been of great concern in the design of CAFE.

A general design for a strategy to use in any system for accessing information is to use general queries and probes to identify a neighbourhood of interest, and then browse and filter [16] (p. 181). This is especially supported in the Curious mode in CAFE. The Curious mode and the other modes can be characterized by their different ways of viewing the information in e-mail. Messages already read and stored represent a collection that is static in its nature. New and unseen messages lying in the inbox or in folders form a semi-dynamic collection of messages, i.e., their state is likely to change in the near future. The incoming messages, finally, form a dynamic collection (a stream) of messages waiting to be classified and acted upon by the user or the system. In other words, we get the following characteristics of the different modes:

- in the Busy mode, we have a semi-dynamic or static deposit of messages (new and unread) on which dynamic, automatically created queries are applied
- in the Cool mode, we have a dynamic stream of messages and a set of static, user-defined queries that are applied to it
- in the Curious mode, we have a static message storage on which dynamic, interactively created queries are applied.

Our aim has been to use simple techniques and metrics, whose function and behaviour can be easily understood by the user—at least intuitively. A prototype of the conceptual model is presented in the next section.

4. The prototype of CAFE

The implementation of CAFE is based on the e-mail client called Exmh [36]. Exmh was originally conceived with the assumption that the user would want to customize it—four ways of customization are available, depending on the desired extent [21]. Moreover, users are allowed to alter and make additions to the source code of Exmh, something which is a major bonus when developing an e-mail client. Exmh has been used as a basis for the development of different extensions by many users [5][38]. Finally, our implementation makes use of known algorithms and techniques in IRIF.

Many people depend on getting e-mail reliably. Furthermore, most people (if not all) do not want the system to automatically delete e-mail without letting the user read it first [29]. Also, you can lose some or all of your incoming e-mail if your automatic e-mail handling is not working correctly or is giving you the right feedback. All

of these issues have been among the central considerations in the implementation. Another consideration has been to not impose a specific mail handling procedure or ordering of actions. However, out of practical reasons this cannot be avoided. For example, in the Busy mode the user will most certainly want to refile some messages for later action, so we added the *ToDo* folder. Each mode uses a different information retrieval (IR) or text categorization technique. In this regard, the modes are described in more detail below.

The Busy mode. The Busy mode is illustrated by fig. 3.

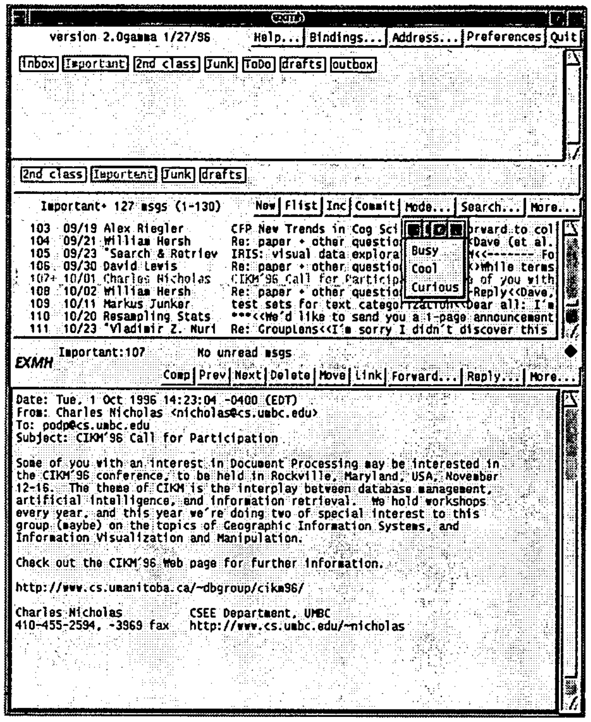


Figure 3. The main window of Exmh, with the Busy mode of CAFE active.

The user is currently browsing the folder containing important messages. The contents of the menu under the Mode button are also shown in the figure. The folder display in the top pane of the window contains the folders used in the Busy mode:

- the three main folders *Important*, *2nd Class*, and *Junk*, representing important messages, second class messages, and junk messages, respectively
- the standard folders *inbox*, *outbox*, *draft*, and *ToDo*, representing incoming messages, outgoing messages, half-completed messages, and messages to be acted upon, respectively.

The routing of messages into the three main folders is done using the text-based Naive Bayesian learning algorithm. The algorithm uses Bayes' Theorem from probability theory. This algorithm makes the computations for training and classification simple, and it also performs rather well in practical applications of classification of text documents—see, for example [19]. It is employed via *ifile*, a filtering program developed by Jason Rennie at Carnegie Mellon University [38]. Messages are prioritized in *ifile* by giving the words on *Subject* and *From* lines higher weights in the computations.

The user can refile messages, either moving wrongly categorized messages into their right folders (folders that are available in the Busy mode) or saving messages for later action in the *ToDo* folder. The learning algorithm updates its parameters accordingly when the user refiles messages to any of the three main folders. However, the refiling of messages to the *ToDo* folder does not affect the algorithm. This is because, learning the system to file messages into the *ToDo* folder borders the area of workflow and work procedures, which are outside of the scope of our work.

Changing to or from the Busy mode changes the folder display. The standard folders (and the *Junk* folder) are used in all modes and remain the same. The messages in the three main folders are automatically moved to the user-defined folders when the user switches to the Cool mode, using the standard filtering rules of the Cool mode. Messages already in *Junk* are not moved, however.

The Cool mode. The folder display of the Cool mode (the top pane in fig. 3) shows the user-defined folders. These folders are used as targets for the user-defined rules that filter incoming messages. Messages that have not been filtered by the rules are left in the *inbox* and can be moved manually to their right folders by the user.

The filter rules are defined by the user in a separate filter file, one rule per line, using a text editor. The syntax of the rules is [21] (p. 374–383):

field pattern action result string

An example of a filter rule looks like this:

from joe qpipe A "/x/y/rcvstore +JoeLetters"

Here, the field argument is *from* and the pattern argument is *joe*, meaning that messages from *joe* will be acted upon. The result argument *A* means that if the field and pattern are matched, an action is performed. In this case, the action is to move the messages to the folder *JoeLetters* (defined in the *string* argument). The action argument *qpipe* is used to start a program. Since the result argument is A, the message is also marked "delivered", which means that it cannot match any more rules. In this example, it starts the *rcvstore* program defined in the string argument, which performs the actual filing of the message. Note that the categories in the

Cool mode are created by the user and separate from those used in the Busy mode (see above).

The Curious mode. Matching the user's need with documents in a collection is a challenge in any IR system. The Curious mode is designed to meet the challenge of "the anomalous state of knowledge", at least to some extent.

The Curious mode uses its own window for the display and selection of groupings of messages (fig. 4). Each grouping is shown in a scroll window of its own. A summary of each grouping is displayed in the header of each scroll window, consisting of the grouping number, the number of messages in it, and the ten most common words in the grouping. To make use of this mode, the user

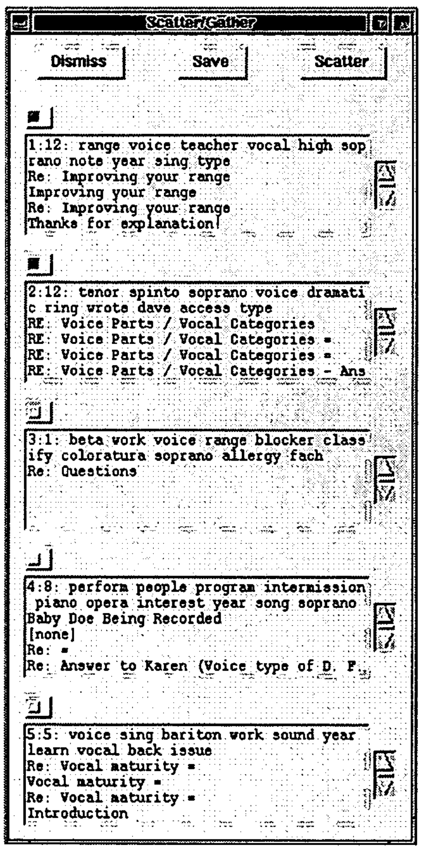


Figure 4. An example of the results of Scatter/ Gather in the Curious mode.

typically selects a set of folders when she is in the Cool mode. The folders of the Busy mode can also be employed. The selection is done via a combination of keys that is consistent with the way Exmh is used. Thereafter, the user changes the mode to the Curious mode via the Menu button in Exmh (fig. 3), opening a separate window on the screen.

The messages are grouped into new categories based on groupings (clusters) that are created by a variant of the Scatter/Gather algorithm [4]. The algorithm uses a non-hierarchical partitioning strategy to cluster n documents into k groups. A strategy called Buckshot [4] is used to find initial centres for the clusters. Buckshot is non-deterministic, i.e., different (random) centres are output each time the same document set is given. The centres are used as starting points in the clustering algorithm that is employed to organize a set of documents into a given number of topic-coherent groups. We use Ward's method, a hierarchical agglomerative clustering method [9]. It uses the minimum variance measure to calculate "closeness" between points (documents). Though it is sensitive to outliers (documents far from the cluster centres), Ward's method produces compact groups of well distributed size and is deemed as appropriate for our domain. The input to the clustering algorithm are a pairwise similarity measure and the number of desired clusters. We use Dice's coefficient, since the documents are short and execution time is critical [26][9]. The number of desired clusters can be set by the user via the Preferences window in Exmh (the default is 5). The assignment of documents to cluster centres is only done twice, since the assignment process makes its greatest gains in the first few steps [4]. The second time, new cluster centres are computed using the m most central documents in each group. We use the 70 % of the documents that are "closest" according to the minimum variance measure used in Ward's method. Since the Scatter/ Gather algorithm is interactive, Buckshot is therefore optimized for speed rather than accuracy (i.e., the rate of misclassification).

4.1 A worked example

Suppose the user has just arrived at her computer and starts her e-mail client (typically by clicking on an icon). Furthermore, suppose she is in a hurry, so she wants to see all important messages among all unseen and new messages. Thus, she changes the mode to Busy (the Cool mode is the default when the e-mail client is started) by selecting the mode from the menu under the Mode button. Now, the important messages are made available in a separate folder named *Important* (fig. 3). After doing some quick reading the user refiles a couple of messages into the *ToDo* folder, some other messages into the *Junk* folder, and another couple of messages into the *2nd Class* folder. The user then exits the e-mail client, since she has skimmed through her new and unseen e-mail and is in a hurry to other places. Note that the filter rules of the Cool mode continue to work in the background and sort incoming messages into the user-defined folders available in the Cool mode.

Suppose the user comes back, now with more time on her hand. Let us say that she is interested in examining the messages from a mailing list called VOCALIST [41] that she has stored in the folder with the same name. The

messages have previously been routed to the folder by the user-defined rules in the Cool mode. The first action that she takes is to mark the VOCALIST folder—she could also have continued to select other folders by using the same marking procedure. She then changes to the Curious mode via the menu under the Mode button (fig. 3).

A separate window for the Curious mode appears, with a message asking the user to wait while the system creates groupings out of the selected folder (or folders) of messages. After a while, the result is shown (fig. 4). Each grouping is shown in a scroll window of its own. A summary of each grouping is displayed in the header of each scroll window, consisting of the grouping number, the number of messages in it, and the ten most common words in the grouping. Let us say that the user is especially interested in "voice types". She selects the groups with summaries containing the words "voice" and "type" (the first two groups in fig. 4) by clicking on the button in the header of the scroll windows. She then clicks the Scatter button to see new groupings of the newly selected messages. In this way, the user iteratively refines the search for interesting messages. When the user has satisfied her information needs, she has the option to save the groupings as new folders, before she quits the Curious mode by dismissing the window.

5. Discussion and conclusion

It is clear that the capability to manage heavy e-mail load is rapidly moving from a an extra feature, to something that is absolutely mandatory.

By examining individuals' categorization processes and organization of messages on the computer screen, we were able to extract a number of interesting concepts and ideas for both an interface an a new conceptual model for handling e-mail messages. The messages can be viewed as either a continuous stream of messages or a stored collection of messages. The conceptual model, a Categorization Assistant For E-mail (CAFE), consists of three modes: the Busy mode, the Cool mode, and the Curious mode. Each mode treats the messages in different ways. Each mode is also used in a different situation, depending on the user's "state of mind" and the amount of time that she has available.

With CAFE, the filtering functions of the e-mail client can be personalized. That is, the sorting of messages into folders (categories) can be done in more than one way. The Cool mode gives the user full control of simple filtering rules. Typically, the messages are sorted into categories that are topic-oriented or sender-oriented, i.e., based on the *Subject* or *From* lines of messages. More advanced rules can be derived via the machine learning algorithm in the Busy mode. The algorithm complements the filtering rules in the Cool mode. With the Scatter/Gather algorithm in the Curious mode the user can first seek broadly relevant information and then browse to reach the goal. Here, the user can make queries that she even cannot state, simply by selecting groups instead of individual queries. Apart from the explorative possibilities, a certain level of serendipity can also be achieved via the Curious mode.

As Marchionini [16] (p. 44) points out, the cost of flexible representations of information is in the various mechanisms for controlling the different representations. The mechanisms—usually paging, scrolling, and jumping—require the user to develop new strategies for manipulating the physical structure of the information, e.g., the length of a message or multiple windows on the screen [16]. In CAFE, in this regard, we have not introduced any new mechanisms not available in the e-mail client Exmh before. For example, the folders are still represented in the same way, i.e., as collections of browsable message summaries in scroll windows.

Our experience suggests that in general, for the user to be able to formulate her information need, a successful implementation should make it possible for the user to use her experience and expertise.

Browsing is a central strategy in accessing information. In a terminology borrowed from Marchionini [16] this strategy can be supported using either *probes*, *filters*, or *templates*. In our prototype:

- the "probes" are represented by the different search functions, such as Scatter/Gather in the Curious mode[1]
- the "filters" are represented by the filtering rules in the Cool mode
- the "templates" are represented by the predefined folders in the Busy mode[2].

The implementation of the hierarchical clustering algorithm (Ward's method) in the Curious mode is currently too slow. Also, two documents with the same content, but written in different languages, are not treated as similar documents, since similarity is based on keywords, which is a drawback of the simple techniques chosen. Furthermore, large clusters should be split into two clusters.

Concludingly, the locus of control is still close to the user in CAFE, who gets a handful of new and usable possibilities of handling her e-mail. Furthermore, we alleviate some of the cognitive demand on the user in refining her "anomalous state of knowledge". Finally, the different modes ameliorate the possibilities to personalize the information management in e-mail.

---

1. Furthermore, Exmh has Glimpse [37] as a built-in search engine.
2. In addition, Exmh uses, among other things, the *components* file for creating templates [21].

6. Future work

The conceptual model can be extended in several ways: more personalized modes resembling user profiles [18] can be added, the data in address book, calendar, and other "add-ons" associated with the e-mail client can also be included in the model. Examples of add-ons are addressing through aliases, adding message signatures, supporting "advanced" text formatting, and spell checking. Information in other domains, such as netnews messages and personal document collections could also be managed. Fleming and Kilgour [8] have described an approach to restructuring the domain of e-mail, deriving message prototypes (templates) directly from users' formal or informal message structures. Incorporating these ideas, which relate to visual programming, can make the conceptual model even more flexible. For example, this could make searches based on message structures [15] such as "review form" and "meeting announcement" possible.

One future direction for our work is generalizing it to other kinds of information and, also, scaling it up for larger volumes of unrestricted text. The Scatter/Gather algorithm was originally designed for large document databases: 30 MB of ASCII text in about 5000 New York Times News Service articles [4].

The Curious mode can be applied to the results of a search with Glimpse [37] in Exmh and thus enabling the user to view the search results in another way [10]. An important part is the definition and handling of the rules in the Cool mode, which really should be done via a special user interface [29]. However, we let the user define and edit the rules in an ordinary text file in the current implementation.

The first concrete goal is to optimize the execution of the algorithms in the prototype and make an evaluation of the prototype with real users. Exmh is used by other persons at our department, which opens up the possibility to make an evaluation of CAFE in a real environment.

There are many optimizations that can be done concerning the execution of the algorithm and the language that it is implemented in (Perl [34]), including changing the language completely for substantial efficiency savings. The initial cluster centres in the algorithm might be selected based on how dissimilar they are, e.g., similarity measure less than 0.05, instead of a random selection. We are considering making the prototype available on the Internet for Exmh users.

Acknowledgments

This paper has benefitted from the comments of four anonymous reviewers. We would also like to thank the subjects who participated in the case study that formed one of the bases for the model. Also, we would like to thank Marie de Korsak and Christophe Millet who implemented the structure editor EFCE for the case study, without which the case study would not have been possible.

References

[1] Belkin, N. J. (1980), "Anomalous States of Knowledge as a Basis for Information Retrieval," in *Canadian Journal of Information Science, 5,* pp. 133–143.

[2] Buzan, T. (1995), *The Mind Map Book.* 2nd ed. London: BBC Books.

[3] Cañas, A. J., Safayeni, F. R., & Conrath, D. W. (1985), *A Conceptual Model and Experiment on How People Classify and Retrieve Documents.* Dept. of Management Sciences, University of Waterloo, Ontario, Canada, April 30, 9 pp.

[4] Cutting, D. R., Karger, D. R., Pedersen, J. O., & Tukey, J. W. (1992), "Scatter/Gather: A Cluster-based Approach to Browsing Large Document Collections," in N. Belkin, P. Ingwersen, & A. M. Pejtersen (Eds.) *SIGIR '92 Proceedings of the Fifteenth Annual International ACM SIGIR Conference on Research and Development in Information Retrieval.* ACM Press, pp. 318–329. ISBN 0-89791-523-2.

[5] Danvind, P. & Mattsson, M. (1996), *Computational Mail.* Master Thesis. Centre for Distance-spanning Technology, University of Luleå, Sweden. `http://www.cdt.luth.se/%7emattias/ex-jobb/report/thesis.ps`

[6] Eberts, R. (1993), "Postmaster: Trainable Neural Net-Based Agents for Sorting E-Mail Messages," in *2nd Industrial Engineering Research Conference Proceedings 1993,* Los Angeles, pp. 534–538.

[7] Eysenck, M. W. (ed.) (1990), *The Blackwell dictionary of cognitive psychology.* Basil Blackwell Ltd, Oxford. ISBN 0-631-15682-8.

[8] Fleming, S. T. & Kilgour, A. C. (1994), "Electronic Mail: Case Study in Task-oriented Restructuring of Application Domain," in *IEE Proceedings: Computers and Digital. Techniques, Vol. 141, No. 2, March 1994,* pp. 65–71.

[9] Frakes, W. B. & Baeza-Yates, R. (1992), *Information Retrieval: Data structures and Algorithms.* Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 504 pp. ISBN 0-13-463837-9.

[10] Hearst, M. A. & Pedersen, J. O. (1996), "Reexamining the Cluster Hypothesis: Scatter/Gather on Retrieval Results," in Frei, H-P, Harman, D., Schäuble, P., & Wilkinson, R. (Eds.) *SIGIR '96 Proceedings of the Nineteenth Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Zürich, August 18–22, 1996.* ACM Press, pp. 76–84. ISBN 0-89791-792-8. `http://www.parc.xerox.com/istl/projects/ia/papers/sg-sigir96/sigir96.html`

[11] Kilander, F., Fåhræus, E., & Palme, J. (1997), *Intelligent Information Filtering.* The IntFilter Project, Dept. of Computer and Systems Science, Stockholm University, Feb. 17, 1997. `http://www.dsv.su.se/~fk/if_Doc/juni96/ifrpt.ps.Z`

[12] de Korsak, M. & Millet, C. (1996), *A Structure Editor for Categorization Experiments.* Master thesis. Dept. of Computer and Information Science, Linköping University, LiTH-IDA-Ex-9631.

[13] Liddy, E. D., Paik, W., & Yu, E. S. (1994), "Text Categorization for Multiple Users Based on Semantic Features from a Machine-Readable Dictionary," in *ACM Transaction on Information Systems, Vol. 12, No. 3, 1994*, pp. 278–295.

[14] Mackay, W. (1988), "Diversity in the Use of Electronic Mail: A Preliminary Inquiry," in *ACM Transactions on Office Information Systems, Vol. 6, No. 4, October 1988*, pp. 380–397.

[15] Malone, T. W., Grant, K. R., Lai, K-Y, Rao, R., & Rosenblitt, D. (1987), "Semistructured Messages Are Surprisingly Useful for Computer-Supported Coordination," in *ACM Transactions on Office Information Systems, Vol. 5, No. 2, April 1987*, pp. 115–131.

[16] Marchionini, G. (1995), *Information Seeking in Electronic Environments*. Cambridge University Press, 224 pp. ISBN 0-521-44372-5.

[17] McElligott, M. & Sorensen, H. (1994), "An Evolutionary Connectionist Approach to Personal Information Filtering," in *Irish Neural Networks Conference '94, University College Dublin, September 12–13, 1994*.

[18] Meadow, C. T. (1992), *Text Information Retrieval Systems*. San Diego, California: Academic Press, Inc., 302 pp. ISBN 0-12-487410-X.

[19] Moulinier, I. (1996), "A Framework for Comparing Text Categorization Approaches," in *AAAI Spring Symposium on Machine Learning in Information Access, Stanford, March 25-27, 1996*. `http://www.parc.xerox.com/istl/projects/mlia/papers/moulinier.ps`

[20] Palme, J. (1995), *Electronic Mail*. Boston: Artech House, 267 pp.

[21] Peek, J. (1995), *MH & xmh: Email for Users & Programmers, 3rd Edition*. O'Reilly & Associates, Inc., 738 pp. ISBN 1-56592-093-7.

[22] Rapp, B. (1993), "Informationshantering på individ- och organisationsnivå," in Ingelstam, L. & Sturesson, L. (Eds.) *Brus över landet*, pp. 117–141. In Swedish. Carlssons Bokförlag. ISBN 91 7798 689 X.

[23] Raymond, D. R., Cañas, A. J., Tompa, F. W., & Safayeni, F. R (1989), "Measuring the Effectiveness of Personal Database Structures," in *International Journal of Man-Machine Studies, No. 31, Sep. 1989*, pp. 237–256. `http://daisy.uwaterloo.ca/~fwtompa/.papers/ijmms.ps`

[24] Rocha, L. M. (1994), "Cognitive Categorization Revisited: Extending Interval Fuzzy Sets as Simulation Tools for Concept Combination," in *Proceedings of the 1994 International Conference of NAFIPS/IFIS/NASA. IEEE Press*, pp. 400–404. `http://ssie.binghamton.edu/~rocha/n94_abs.htm`

[25] Rosch, E (1978), "Principles of Categorization," in *Cognition and Categorization*, E. Rosch, B. B. Lloyd (Eds.), Lawrence Erlbaum Associates, Hillsdale, New Jersey, pp. 27–48. ISBN 0-470-28377-6.

[26] Salton, G. & McGill, M. J. (1983), *An Introduction to Modern Information Retrieval*. New York: McGraw-Hill, 448 pp. ISBN 0-07-054484-0.

[27] Smith, E. (1990), "Categorization," in Osherson, D. N. & Smith, E. (eds.) *An Invitation to Cognitive Science, Vol. 3, Thinking*. MIT Press, pp. 33–53. ISBN 0-262-15037-9.

[28] Sproull, L. & Kiesler, S. (1991), *Connections: New Ways of Working in the Networked Organization*. Second edition. MIT Press: Massachusetts, 212 pp. ISBN 0-262-19306-X.

[29] Takkinen, J. (1994), *CASUAR – en prototyp av ett användargränssnit med filtrering och automatik för hantering av elektronisk post*. In Swedish. M.Sc. Thesis, Linköping University, Sweden, 126 pp. LiTH-IDA-Ex-9445. `http://www.ida.liu.se/~juhta/publications/publications.html`

[30] Takkinen, J. (1995), "An Adaptive Approach to Text Categorization and Understanding," in *Conference Proceedings 1995, 5th Annual IDA Conference on Computer and Information Science, November 22, 1995*, Department of Computer and Information Science, Linköping University, pp. 39–42.

[31] Takkinen, J. (1997), *Categorization of unrestricted text: towards a conceptual model for information management in electronic mail*. Licentiate Thesis No. 640, Dept. of Computer and Information Science. `ftp://ftp.ida.liu.se/pub/publications/lic/1997/0640/`

[32] Tijsseling, A. G. (1994), *A Hybrid Framework for Categorization*. Master Thesis, Dept. of Cognitive Artificial Intelligence, Faculty of Philosophy, Utrecht University. `http://www.soton.ac.uk/~coglab/coglab/Thesis/`

[33] Vickery, B. & Vickery, A. (1992), *Information Science in Theory and Practice*. London: Bowker-Saur. ISBN 0-408-10684-0.

[34] Wall, L., Christiansen, T., & Schwartz, R. L. (1996), *Programming Perl*. O'Reilly & Associates, Inc. ISBN 1-56592-149-6.

World-Wide Web URLs

[35] *BeyondMail*. `http://www.coordinate.com/`

[36] *Exmh*. `http://www.smli.com/~bwelch/exmh/index.html`

[37] *Glimpse*. `http://glimpse.cs.arizona.edu/`

[38] *The Official ifile Web Site*. `http://www.cs.cmu.edu/%7ejr6b/ifile/`

[39] *Intelligent Instruments for Information Management*. Project description, Dept. of Informatics, Göteborg University. `http://www.adb.gu.se/~janl/III.eng.html`

[40] *Ishmail User's Guide*. HAL Computer Systems, Inc., Campbell, California, USA, October 1995. `http://www.ishmail.com/`

[41] *VOCALIST*. `http://lists.oulu.fi/vocalist/`

[42] *Z-Mail*. `http://www.netmanage.com/`

A secure Email gateway (building an RCAS external inter

Smith, R.E.
Boeing Co., Seattle, WA, USA;

This paper appears in: **Computer Security Applications Conference, 1994. Proceedir**
Publication Date: 5-9 Dec. 1994
On page(s): 202 - 211
Meeting Date: 12/05/1994 - 12/09/1994
Location: Orlando, FL
INSPEC Accession Number:4852779
Digital Object Identifier: 10.1109/CSAC.1994.367307
Posted online: 2002-08-06 19:20:42.0

Abstract
Fielding secure computer systems requires tradeoffs between functionality, flexibility, anc users' needs. Multilevel secure (MLS) computer systems provide better control over class traditional systems and allow users from a diverse population access to information they sensitive data. Users want the functionality of non-MLS computer systems; graphical use assortment of software, and electronic connectivity with other systems. Compartmented r (CMW) can provide such an environment. An overview of secure system architectures ar **network** provide the framework for discussing the risks associated with interconnecting M unclassified **networks**, and approaches for mitigating those risks. A secure Email gatewa assurance (AI) **network** component, provides the necessary safeguards for protecting th external attacks

Index Terms
Inspec
Controlled Indexing
electronic mail internetworking multi-access systems **security** of data

Non-controlled Indexing
MLS **network** RCAS external interface classified informatio compartmented r workstations diverse population electronic connectivity example MLS **networ** attacks graphical user interfaces high-assurance AI **network** component mul computer systems secure Email gateway secure computer systems secure s architectures unclassified **networks** user needs

Author Keywords
Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEE Xplore.

A Secure Email Gateway (Building an RCAS External Interface)

Randall E. Smith
The Boeing Company

Abstract

Fielding secure computer systems requires tradeoffs between functionality, flexibility, and security to meet the users' needs. Multilevel secure (MLS) computer systems provide better control over classified information than traditional systems and allow users from a diverse population access to information they need while protecting sensitive data. Users want the functionality of non-MLS computer systems; graphical user interfaces, a rich assortment of software, and electronic connectivity with other systems. Compartmented mode workstations (CMW) can provide such an environment. An overview of secure system architectures and an example MLS network provide the framework for discussing the risks associated with interconnecting MLS systems and unclassified networks, and approaches for mitigating those risks. A secure Email gateway, using a high-assurance (A1) network component, provides the necessary safeguards for protecting the MLS network from external attacks.

1: System-High, Parallel, or MLS

Separation of information based upon classification has traditionally been accomplished by assigning a security classification to the information, creating a physically secure perimeter around the information, and requiring appropriate security clearances of all persons needing access to this information. Such "system-high" environments ignore the different classifications of the data by requiring that all data protected by the system be treated as though it is classified at the highest level authorized for the system. Only a person with a clearance that dominates (is the same or higher than) the security classification of the most sensitive information protected by the perimeter is allowed to enter. Once inside the perimeter, access is granted only to the specific information that the person needs. Electronic data processing systems (i.e., computers) used within a system-high computer network traditionally do not provide the mechanisms or the assurances necessary to identify the security level of each piece of its information or to guarantee that information at a lower classification cannot become contaminated by information of a higher classification. As a result, all information imported into a system-high computer must be treated as though it contained information at the system's highest level. In Figure 1, unauthorized users are not allowed into the security perimeter and unreviewed data is not allowed out.

System-high environments work well if all people needing access to the data are already cleared at the highest level of the system and if the data is not exported to a system with a lower classification. The procedures used for validating the security level of information stored in a system-high computer when the information is exported are both time-consuming and unreliable, and

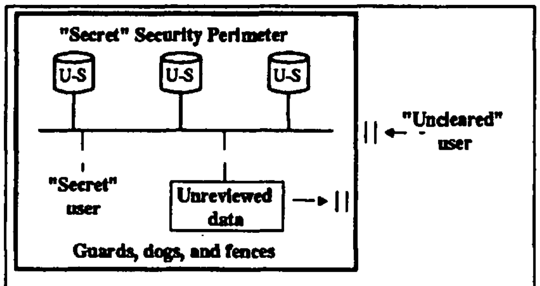


Figure 1. System-High Environment

are unnecessary if the computer system is trusted to maintain the identification and separation of the classified information. System-high computer systems also ignore the real needs of users by requiring security clearances (at considerable expense), even for those who will never need access to classified data.

Some drawbacks associated with system-high environments are addressed by using multiple, single-level computer systems as shown in Figure 2. In this environment, a Secret, system-high computer network and an unclassified computer network coexist so that the users are assured that the unclassified information (stored on the unclassified network) always remains unclassified. Computers and terminals connected to the unclassified network may be located in unsecured areas and accessed by uncleared persons without fear of compromising the Secret computer system. Problems arise when a user needs to incorporate information from both systems into

1063-9527/94 $4.00 © 1994 IEEE

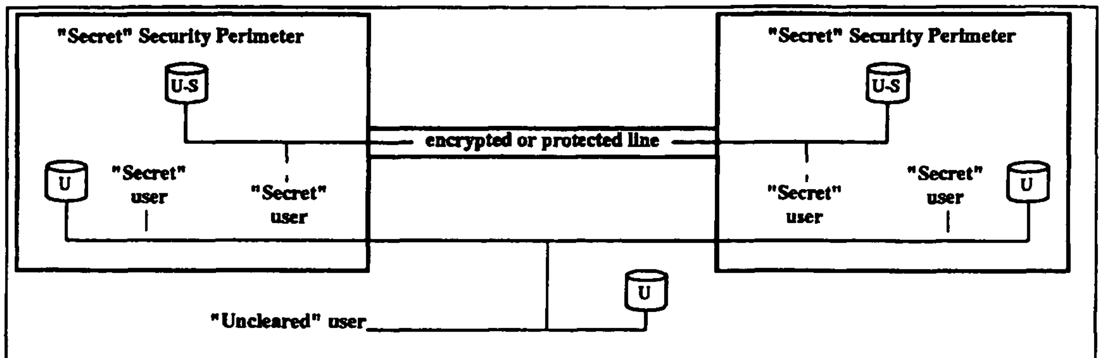


Figure 2. Parallel Network Environment

a single document. It may be necessary to include unclassified information from a Secret document in an unclassified report, or to include unclassified information from an unclassified document in a Secret report. The procedures for moving data from one system to another are not convenient and may require re-entering the data manually. Fielding multiple single-level networks also has its drawbacks due to the expense of the duplicate equipment. This scheme is unattractive to users who must access data stored on both networks because they must switch between multiple terminals to accomplish their job. These drawbacks increase as more types of classified data (e.g., Top Secret or special access) are introduced into the environment.

The solution resides in building computer systems with sufficient features and trust to appropriately label all information with the appropriate security classification and keep the information separated while allowing access only to those persons authorized for the data. The National Computer Security Center (NCSC) published the Trusted Computer System Evaluation Criteria (TCSEC) [1] to categorize computer systems based on the features and assurances they provide to protect sensitive data. The NCSC evaluates computer products against the criteria contained in the TCSEC and publishes its results in their Evaluated Products List (EPL). A series of related documents provide guidelines for applying the standards of the TCSEC to computer products. MLS systems are evaluated against the TCSEC criteria for B1, B2, B3, or A1 ratings. Computer networking components are also evaluated using the guidance of the Trusted Network Interpretation (TNI) [2]. The functional differences between the lowest MLS rating of B1 and the highest rating of A1 are minimal; however, the probability that security flaws exist in the system decrease dramatically as the system rating goes from B1 to A1. Most of the differences between B1 and A1 systems are found in the way they are designed, architected, analyzed, and tested. The higher the evaluation rating, the better the system is at assuring that the security policy enforced by the system cannot be compromised.

The parallel network configuration from Figure 2 can be re-architected by using MLS technology to provide the appropriate data to authorized users in approved locations without the problems of duplicated equipment or manual downgrade between system. This redesigned MLS configuration is shown in Figure 3. Each MLS computer is configured to protect an appropriate range of data and each interface into the computer is likewise assigned a security range. In this environment, an uncleared user outside of the physically-secured Secret and Confidential facilities is still able to access unclassified information from all three computer systems shown without being able to access any classified information. Users within the Confidential security perimeter can likewise access any unclassified information, but are also able to get to any Confidential data in their own facility or the Secret facility, if necessary. Users in the Secret facility have access to all of the information stored within the MLS computer system.

2: Problem Definition

Users within the Department of Defense (DoD) want the same capabilities found in today's commercial, off-the-shelf (COTS) products but must have access to both unclassified and classified information. Few high-assurance components (B3 or A1) exist today and these do not yet support the rich suite of applications available for non-MLS computer systems (e.g., graphical user interfaces and integrated office automation software). CMWs provide users with a graphical user interface (trusted X windows), a widely-used operating system

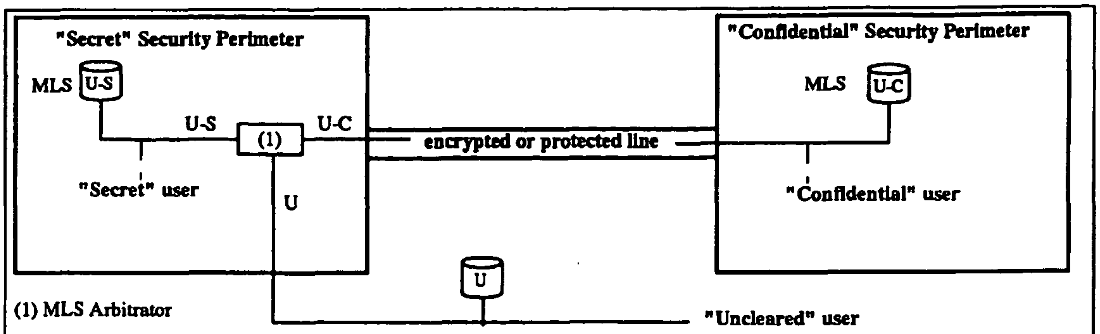


Figure 3. MLS Networking Example

(UNIX) rich with COTS applications, and the ability to work within an MLS environment (at the B1 level of assurance). We look at one example of a very large MLS network to examine the issues related to MLS computer systems.

The United States Army and National Guard units are currently undergoing a dramatic change in the way they perform their duties [3]. The Reserve Component Automation System (RCAS) consists of computer hardware and software being fielded to provide a common, integrated suite of office automation tools electronically linking all of the units. Additionally, a number of RCAS applications are being developed to electronically replicate the paper forms system currently in use [4]. RCAS must interconnect military computer systems at over five thousand sites scattered throughout the United States. These sites are connected with end-to-end encryption over both dedicated and dial-up lines and rely upon electronic mail as the primary communications service between sites.

Like many DoD computer systems, RCAS contains mostly unclassified information; however, some classified data must also be accessible to those with both the necessary clearance and need for the data. Running RCAS as a Secret, system-high network was ruled out because it would require extensive site modifications and Secret clearances for all of the Army Reserve and National Guard personnel. A parallel network architecture was also considered, but RCAS was designed and fielded as a multilevel computer system in order to provide the required functionality, notably a user must be able to perform all functions from a single point of entry.

As an MLS network, RCAS was required to comply with government regulations specifying the trustworthiness of computer components when selecting the equipment. The NCSC publishes the *Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environment* [5], or the "Yellow Book", for use in determining the appropriate ratings (B1 through A1) needed by computer components used in MLS systems. Table 1, below, presents a concise summary of the Yellow Book's guidance based upon the highest classification of data protected by the system and the lowest clearance level of a potential user of that system. The rows in the table represent the minimum clearance needed by a user of the system. The columns represent the highest classification of data protected by the system. The intersection of a row and a column identifies the minimum trust (TCSEC category) required for the system. It is clear from this table that a rating of B1 or higher is required whenever the minimum user clearance is less than the highest data classification; however, there are few cases where a B1 system is sufficient. There are also environments identified by the Yellow Book where the NCSC believes that even the protection of an A1 system is inadequate.

RCAS meets the Yellow Book's guidelines by using a B1 computer system, accessible by personnel with at least a Confidential clearance, to protect data classified at no higher than Secret. Many DoD computer systems have similar user and data requirements and could benefit from the advantages of a CMW architecture. But what happens when you must exchange data with another computer system where the potential users of one system do not meet the clearance requirements of the other system? Some additional procedures, controls, or security assurances are needed.

3: Analysis of the Problem

People served by today's computer networks do not exist in isolation. They must be able to communicate with other computing systems. Before the introduction of MLS systems, the only secure way to interconnect systems at different security levels was through an "air gap" between the systems - copy the information off one system and then onto the other system. Some systems

Minimum Clearance or Authorization of Systems' Users		Maximum Data Sensitivity (Evaluation Level): U	N	C	S	TS	1C	MC
Uncleared or Unclassified User	U	C1	B1	B2	B3	*	*	*
Not cleared but authorized access	N	C1	C2	B2	B2	A1	*	*
Confidential User	C	C1	C2	C2	B1	B3	A1	*
Secret User	S	C1	C2	C2	C2	B2	B3	A1
Top Secred (background investigation)	TS(BI)	C1	C2	C2	C2	C2	B2	B3
Top Secret (special background investigation)	TS(SBI)	C1	C2	C2	C2	C2	C2	B2
One Category	1C	C1	C2	C2	C2	C2	C2	B1
Multiple Category	MC	C1	C2	C2	C2	C2	C2	C2

* Future requirements to be defined by NCSC

Equipment Evaluation Ratings

Table 1. Security Index Matrix

were configured to provide a "one-way" write-up from the low system to the high system while blocking any transmission going in the other direction. Others required a person in the loop to manually review all information as it passed through the data exchange point. MLS computer systems provide the capability to directly interconnect systems at different security levels provided the MLS system architecture satisfies the requirements of both systems. If the MLS computer system does not provide enough assurance, as in Figure 4, then an additional device may be needed between the computer systems to provide additional protection.

As shown above, B1 CMWs do not provide the assurance necessary to reliably separate Secret data from uncleared, potentially unknown users. Given an MLS network with all users cleared at least to the Confidential level, and a C2, unclassified network, it is unlikely that a direct electronic connection will meet the security needs of either system. The MLS network must have additional protection from the uncleared users of the C2 network. It is necessary to analyze the security risks involved before

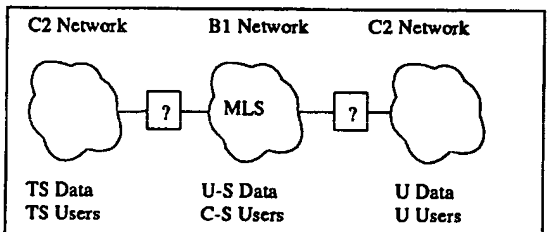


Figure 4. Connecting Computer Systems

an acceptable solution to this interfacing problem can be identified. The following risks were identified as key concerns in the case of the RCAS network:

1. unauthorized access to the MLS network,
2. accidental disclosure of classified information from the MLS network, and
3. malicious software imported into the MLS network.

Access to the RCAS system is controlled by the identification and authorization mechanisms of the CMWs. These mechanisms are implemented by validating a user's name and password before access is granted. Because the RCAS user group is restricted by physical means to a closed set of known users, additional measures (e.g., smart cards or scanners) are not required. Adding an external interface to MLS network presents the problem of unknown, uncleared persons attempting to gain access by guessing user account names and passwords. There have been many highly-publicized examples of successful attacks on interconnected computer systems are known. In one example [6], Bill Cheswick describes watching and trapping an intruder who believes he has accessed a classified military computer by successfully guessing username/password combinations. Bill concludes that "if a hacker obtains a login on a machine, there is a good chance he can become root sooner or later. There are many buggy programs that run at high privileged levels that offer opportunities for a cracker. If he gets a login on your computer you are in trouble." This form of attack must be prevented with a high degree of assurance if unauthorized (or unknown) people can attempt to gain access into the MLS computer system.

Accidental disclosure of classified information can be caused by careless users or by flaws in the security mechanisms of the computer systems. These problems become worse when an attacker enters the system and is then able to exploit the real user or security flaws to trick the system into disclosing additional unauthorized information. An unclassified external interface introduces the possibility of Secret data falling into the hands of uncleared personnel. The external interface must not only prevent the attacker from getting inside the MLS network, but must also minimize and control the paths that could result in classified information leaking out to the external system. Any paths that cannot be closed must be identified and their risks understood.

Virus and Trojan horse software compromise the integrity and security of computer systems. The concern to RCAS is that an unknown person may attempt to insert this type of software into RCAS via an external system interface. Many paths are available in UNIX computer systems for installing executable code. Some methods require accessing an existing account on the computer, while others rely on system services or flaws to create openings. Cliff Stoll details many techniques used by the wily hacker [7]. Not all attacks come directly from an attacker. A program released by an attacker can work its way through the maze of computers looking for weaknesses. One technique used by the Internet worm [8] involved exploiting a debug "feature" of the sendmail program to gain information about neighboring computers. This type of threat must be addressed by any interface into the secure computer system.

4: Searching for a Secure Solution

A team of experts was called to brainstorm a set of desires expressed by the RCAS user community, not the least of which was Email connectivity with non-RCAS computer systems. Three approaches were identified by the team to solving this type of interface problem:

1. Upgrade the CMW network to provide higher (B2 or above) assurance,
2. Interconnect the CMS network to external systems with B1-assured gateways,
3. Interconnect the CMW network to external systems with higher (B2 or above) assurance gateways.

The first approach was the preferred solution. Unclassified computer systems with uncleared (but authorized) users could be directly connected to the CMW network while maintaining the security assurances required by the Yellow Book. There were, however, three problems with this approach. First, there were no COTS products available providing the required functionality (able to run an integrated office automation suite of software, GOSIP-compliant, etc.) evaluated by the NCSC at the B2 level of assurance. Second, most of the currently evaluated MLS products did not include the networking protocol stack (TCP/IP, or TP4/CLNP) as part of their evaluated product. Third, users of an external computer system may be unauthorized, increasing the requirement to at least the B3 level of assurance.

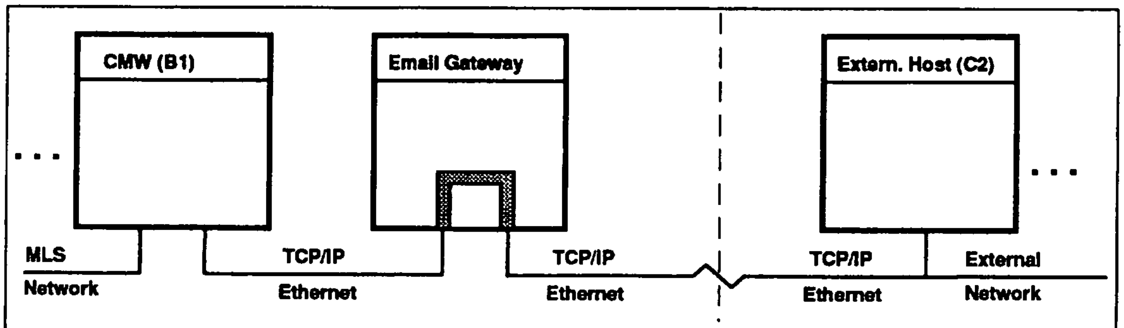


Figure 5. Email Gateway Configuration

The second approach involved configuring an existing RCAS CMW as an Email gateway (See Figure 5). This gateway would disable all non-Email services and provide selective filtering of Email messages based upon configurable parameters. Unauthorized access to the gateway would be controlled by not allowing user accounts and by disabling any interactive daemons that an attacker could exploit. Accidental disclosure of classified information would be handled by reducing the number of paths (services) out of the CMW network (only SMTP service). Introduction of malicious software into the CMW network would be controlled by scanning Email message header fields for specific characteristics

(e.g., messages to pipes or files) and by disabling services that an attacker would normally use to insert software (e.g., TELNET, FTP).

This approach provides the necessary functionality, but concerns were raised about the trustworthiness of a B1 solution. Restricting a B1 computer to the a minimal set of processes needed to implement the gateway does not increase the B1 computer's security assurance to the same level as a B2 or B3 platform. It was believed that attempts to penetrate the CMW network by bypassing the security mechanisms of the gateway, or attempts to compromise the gateway itself and then use it to attack the CMW network, had a high probability of success.

The third approach involved configuring a COTS B2 platform as the Email gateway. This solution has all of the advantages of the B1 solution along with some additional assurance that the gateway would resist more aggressive attacks. One drawback to this solution is the small number of evaluated B2 (or higher) products available that could be used for the gateway platform. An analysis of the available platforms was needed, along with the effort required to create the gateway. Additional information was needed about how the gateway would block the identified threats, and how any residual risks could be mitigated.

5: Problem Revisited, a Candidate is Found

Building an Email gateway using a general-purpose MLS host computer looked like a straight-forward task, but a closer look provided some useful insight. B1 computer products differ from C2 (non-MLS) computer products primarily in the functionality provided to support mandatory access controls. Security labels, user and device access ranges, auditing, and the concept of a Trusted Computing Base (TCB), comprise the major changes to the system. What is provided by B2 through A1 products but lacking in B1 products are the assurances (structuring and minimizing the TCB to support more rigorous architectural analysis and testing, formal specifications, code-to-specification mappings, even informal or formal proofs of correctness) that if the component starts in a secure state, it will remain secure.

Without these added assurances, it is likely that the same flaws found in today's general-purpose computers also exist in the current B1 products. The very nature of a general-purpose computer implies that its configuration is easily modifiable, providing numerous ways an attacker can change the state of the computer. The large size of the TCB software in a B1 computer makes it difficult (if not impossible) to identify and understand all of the possible vulnerabilities available to an attacker. Building a secure Email gateway with this type of an architecture leaves many potential security holes unrelated to the gateway application itself.

We were trying to maintain the security of the system while satisfying the desires of the users by developing a high-assurance application using a low-assurance, reprogrammable MLS product with an unevaluated protocol stack and then trying to convince ourselves it was trustworthy enough. The ideal solution was to integrate a dedicated high-assurance gateway application into a high-assurance, non-reprogrammable, trusted MLS protocol stack. The A1-evaluated Boeing Multilevel Secure Local Area Network (MLS LAN) proved to be an ideal host for developing the Email gateway.

The MLS LAN is a data communications network system component determined by the National Security Agency to fulfill the A1 requirements for mandatory

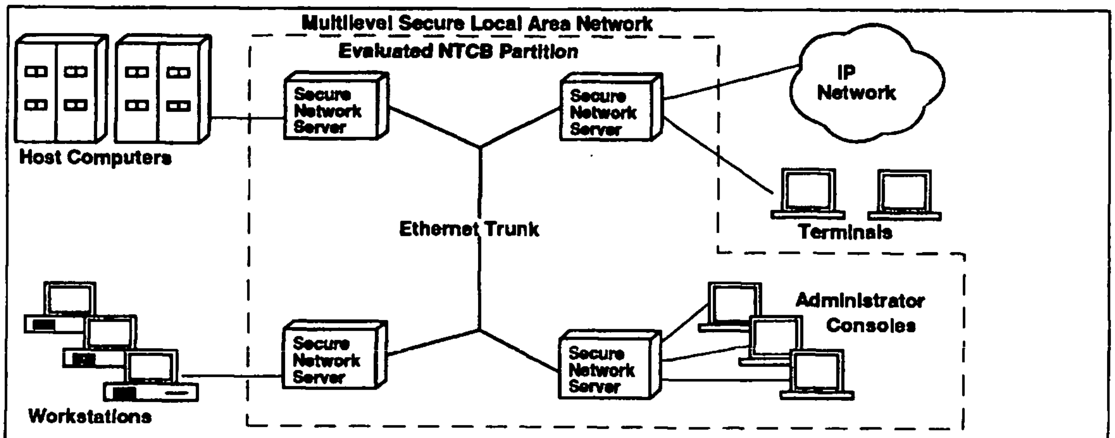


Figure 6. MLS LAN Network Configuration

access control, discretionary access control, identification and authentication, and audit, as defined in Appendix A of the TNI. The MLS LAN provides access-controlled communications between attached devices where these devices may be operating at different sensitivity levels. The MLS LAN is comprised of multiple Secure Network Servers (SNS), a transmission medium, and an SNS configured as a Network Management node (Figure 6). The A1-evaluated MLS LAN product provides many additional capabilities not discussed in this paper. For a complete description of the product, the interested reader should obtain a copy of the NCSC Final Evaluation Report [9].

The basic unit of the MLS LAN is the SNS, which is expandable to support various configurations of multilevel or single-level (labeled or unlabeled) devices. Security labeling over the IP interface supports the Common IP Security Option (CIPSO) [10] protocol. The security label of every datagram is checked as it enters the SNS. Security labels are removed from datagrams before they are sent to unlabeled interfaces, and are added when they are received from unlabeled interfaces.

The security model of the MLS LAN architecture relies upon the separation of processes. Inter-process communications, task scheduling, and hardware interface accesses are controlled by the security kernel and the processor's hardware protection mechanisms. Processes outside of the network trusted computing base (NTCB) are further restricted to a subset of the kernel services. All processes are pre-defined with their code, the initial

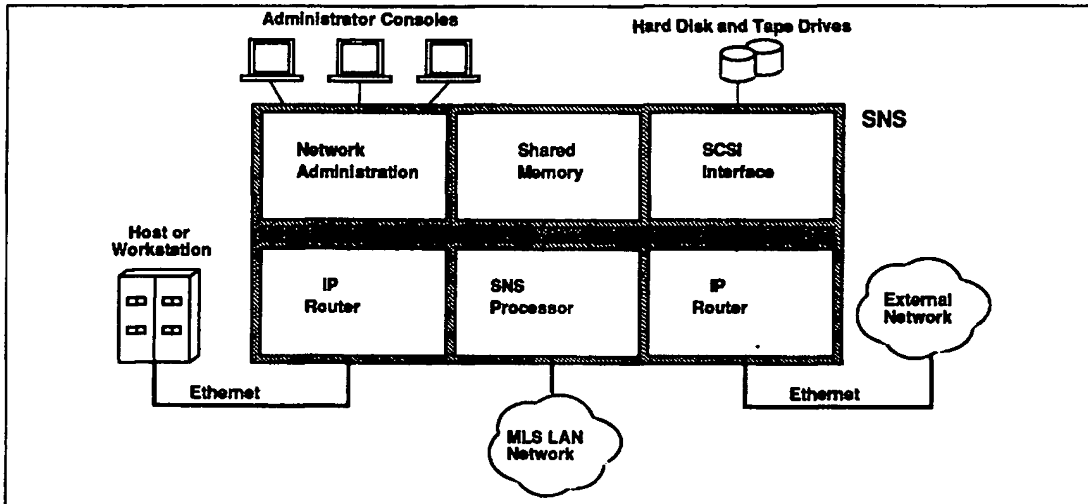


Figure 7. MLS LAN SNS, IP Router Configuration

subscriber devices. The core SNS is comprised of a chassis with shared memory board and an SNS processor (SNSP) providing the Ethernet trunk interface. To achieve a desired level of functionality, subscriber device interface cards are added to the core SNS. A combination of hosts, video devices, and/or terminals can be connected to SNSs in various configurations. Of specific interest for the RCAS gateway is the IP interface card. This configuration provides static routing of IP datagrams from host to network or from network to network (Figure 7).

Hosts or remote networks that use the IP protocol may be connected to an SNS over an interface. IP interfaces may be configured as a host or router interface providing standard IP service. They can be configured as either value of the data and special segments, and all initial memory requirements known at system build time. Dynamic process creation is handled by a template mechanism with only a common code segment and constant, read-only data are shared among processes. Separate read/write data, stack, and special system segments are allocated and initialized from the template for each dynamically created process. There is no mechanism for modifying or adding code to the MLS LAN. Figure 8 shows how the MLS LAN software is partitioned on a typical device interface processor.

An MLS LAN must include one SNS designated as the Network Management (NM) node. This node includes network management software that maintains the network configuration database, supports dynamic

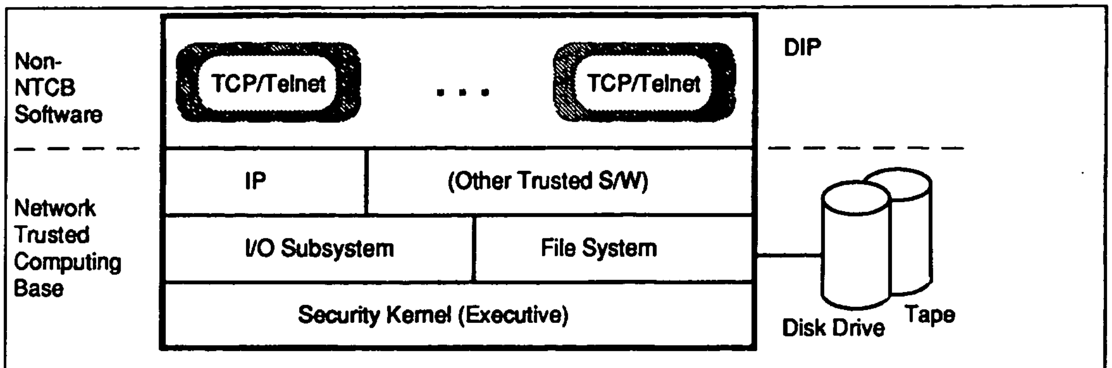


Figure 8. Device Interface Processor Software Architecture.

network reconfiguration, collects audit records, supports network troubleshooting, provides administrator console interfaces, and allows tape backup of configuration and audit information. All network administration functions are supported by NM-attached consoles and are not accessible via network-attached hosts or terminals.

Each SNS also includes one card that handles the configuration, audit, and monitor data between the NM node (or the local NM processor card) and the rest of the cards within an SNS. This card, called the SNS Processor (SNSP), also provides the internet protocol processing, packet labeling, mandatory access control validation, and the trusted components of TCP (multiplexing, demultiplexing, and addressing) for the MLS LAN network. A separate device interface processor can be added to an SNS to provide an interface between an MLS LAN network and an IP host or an IP network. When configured as an IP router, this interface maintains a virtual connection table, discretionary access control (DAC) tables, and an address resolution protocol (ARP) table. It also utilizes the network routing table, security labeling information, and other configuration parameters downloaded from the Network Management node at initialization time.

The MLS LAN supports terminals, hosts, and workstations by adding subscriber device interface processors to the SNS. The host interface processor supports multiple host users by spawning separate, single-level protocol modules to support each connection request. This allows users to create multiple TELNET sessions over the MLS LAN network. These sessions may be created at different security levels based upon the user's clearance, the security range assigned to the user's host, and the security range (or level) of the remote host.

While this protocol software was developed to the same standard as the rest of the MLS LAN software, its correct operation is not required for maintaining the security of the network. In keeping with the high-assurance requirements of the TCSEC, specifically TCB minimization, this protocol software was placed outside of the NTCB. Because it is outside the NTCB, it can be modified or replaced without affecting the A1 rating of the MLS LAN.

What makes the MLS LAN unique is the high degree of confidence that classified information within its network will not be compromised [11]. In addition to the functional requirements of MLS products, an A1-evaluated product must be architected so that the security relevant code can be analyzed, understood, modeled, tested, and verified. The TCSEC defines the A1 assurance requirements for system architecture, system integrity, covert channel analysis, trusted recovery, security testing (including vendor testing, evaluation team functional testing, and penetration testing), design specification and verification (including a formal model, descriptive top-level specification, formal top-level specification, and specification-to-code mappings), trusted distribution, and configuration management. This degree of assurance is not possible with the architecture and size of today's B1 and B2 products.

6: Designing the Email Gateway

The evaluated MLS LAN product provides much of the desired functionality for the gateway. As a high-assurance, non-user reprogrammable system, it represents the best protection available against direct attacks. The MLS LAN's IP DAC feature makes it possible to configure two IP interfaces so that only the TCP Email (SMTP) port is available, while eliminating interactive services like TELNET and FTP. The IP DAC capability can also be used to control which hosts are allowed to use the gateway: in the case of RCAS, only one host on either side of the gateway is allowed access. The threat of unauthorized access to RCAS is effectively

eliminated by the gateway. The SMTP mail service is the only path for accidental disclosure, or insertion of malicious software, and an attacker will be unable to modify the gateway's configuration to create additional paths. The key advantages of this solution are that the potential paths for compromising the RCAS system are reduced to a minimal set and the solution provides high assurance that it can protect itself against compromise.

Some additional protection was needed to prevent attacks directed at the RCAS process (sendmail) that services the TCP mail port. Numerous security flaws have been exploited in the past by using features of the sendmail program and it is naive to assume that new techniques will not be discovered. One recent example discussed on the Internet involved sending mail to pipes (executable programs) or files. These kinds of threats must be handled administratively at each site. Any penetration attempts of this type could not be blocked by the MLS LAN IP router interface without some modification.

Another concern was that an uncontrolled Email interface to "the rest of the world" would invite a flood of unwanted junk mail. It was feared that if user access was not controlled, then anyone from the outside could attempt to use the Email path to insert Trojan horse or virus software into RCAS. Therefore, some controls were needed to define the set of users who would be allowed to send and receive mail through the gateway.

Some extensions to the evaluated MLS LAN product were needed to provide this additional insulation between the two networks. Using the concept of multiple, single-level software protocol modules (much like that used for TELNET/TCP) we added an SMTP component to the IP router software. We minimized the impact of this software on the security of the MLS LAN by building it outside of the NTCB. A new process is spawned for each TCP Email session request and is assigned the same security label as the TCP connection. This process receives the header and body of the mail message, validates it against a set of NM-configured parameters, and stores it within the gateway until the connection is closed. When the mail transaction is complete, the first SMTP process is terminated and a second process is spawned to forward the mail to the destination host. The second SMTP process is created at either the security level of the Email message (the same as the first SMTP process) or at the level of the receiving host if the host's minimum level is higher than that of the data. This design is similar in concept to a low-to-high guard described by Michelle Gosselin [12] except that the allowed application layer protocols are restricted to SMTP, the A1 platform is more resistant to penetration, and the networking protocol stacks are included as part of the evaluated product.

The two-stage, short-term store-and-forward sequence insures that an attacker cannot create an interactive connection directly with the process servicing the SMTP port on an RCAS CMW. Although not currently part of the RCAS plan, this design make it possible to use the Email Gateway to perform blind Email write-ups from a low system to a higher level system (e.g., from the B1 MLS network to the Top Secret network, Figure 4), while preventing covert information from flowing back to the low side from the high side.

Access control lists (ACL) were added to restrict the users of the gateway by defining the set of mailboxes (e.g., user@host) allowed or excluded from sending or receiving mail through the gateway. SMTP mail sessions identify the receivers of the mail in "rcpt_to:" commands and identify the send in the "mail_from:" command. The entire mail transaction is rejected if the sender is not authorized by the sender ACL. An "unknown user" response is returned for any receivers not authorized by the receiver ACL, and they are deleted from the list of

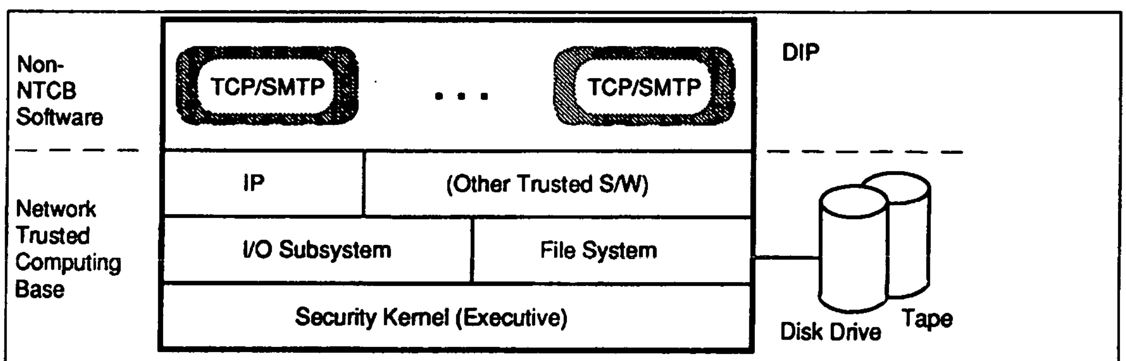


Figure 9. Email Gateway Software Architecture

receivers forwarded to the receiving host. The administrator can also specify that the sender and receiver fields do not address processes, files, or relays.

The "data" section of the SMTP transaction consists of the RFC-822 header followed by the body of the mail. Some header fields are used to route undeliverable mail back to the sender. Error rejections present a security problem if the errors can be routed to processes or files on a targeted host. These header fields (errors-to:, from:, resent-from:, sender:, resent-sender:, and return-receipt-to:) are checked to verify that the targeted host is an authorized host on the originating side of the gateway. Attempts to send rejections to processes, files, or relays can also be checked. Mail rejected by the gateway are returned to the sender in the usual RFC-822 manner, except in the case of a low-to-high write-up, where the response could transmit classified information back to the original sender. No response is returned to the low side.

Some other minor changes to the MLS LAN were needed to support the Email gateway. The network management software was modified to support user access control lists, the new Email gateway device configuration parameters, and new audit events, and the MLS LAN's internal hard disk file system was modified to add a second partition for temporarily storing the Email data.

7: Is it Good Enough?

The A1 Email gateway provides the capabilities needed by RCAS to exchange Email with external unclassified computer systems while protecting itself from attacks. Although it will be used to connect unclassified external systems to an unclassified port in RCAS, could be used to connect Confidential, Secret, or MLS computers to RCAS. The A1 Email gateway is being designed and tested to withstand even the most sophisticated attacks without compromising its security.

Can the gateway keep unknown people who gain access to the external system from attacking RCAS? It certainly minimizes the types of attacks that can be attempted, but part of the responsibility still resides inside the MLS network. Interactive attacks aimed at trying to find user account names and passwords and then using this information to log into the computer (a common technique used by attackers) are not possible through the gateway. Trojan horse and virus software cannot gain entrance through FTP or similar file transfer protocols. Use of Email to insert Trojan horse or virus software into the MLS network requires the cooperation of the person receiving the Email to activate the software. The risk still remains that information from inside the MLS network could leak out in an Email message through the gateway. Education, policies, and procedures are still the best ways to reduce this risk until higher assurance platforms are developed that support general purpose, COTS application software.

Developing RCAS as a very large, distributed MLS system using CMWs, secure OSI communications protocols, an integrated suite of office automation software, and custom RCAS applications to replace paper forms, pushes the technology of secure computing beyond anything previously fielded. High-assurance MLS components, like the A1 Email gateway, can be used to extend the capabilities of secure computer systems and are becoming an important part of MLS computer systems. This trend will continue as the use of MLS computer equipment grows, however, we recognize that high-assurance components like the A1 Email gateway described in this paper cannot protect low-assurance, MLS systems from their own weaknesses. The ultimate solution for B1 networks like RCAS must eventually include an upgrade of the computing equipment to provide a higher level of security assurance.

References

[1] *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Dec. 1985.

[2] National Computer Security Center, *Trusted Network Interpretation*, NCSC-TG-005,31 July 1987.

[3] Christopher Raven, *The Army Reserve's War on Paper*, Uniforum Monthly, April 1994.

[4] Mark O. Aldrich, *A Methodology for the Use of Single Level RDBMS Software in a Multi-level Secured System*, Ninth Annual Computer Security Applications Conference, Orlando, Florida, Dec. 1993.

[5] DoD Computer Security Center, *Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, CSC-STD-003-85, 25 June 1985.

[6] Bill Cheswick, *An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied*, AT&T Bell Laboratories.

[7] Clifford Stoll, *The Cuckoo's Egg*, Doubleday, New York, 1989.

[8] Mark W. Eichin and Jon A. Rochlis, *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988*, Massachusetts Institute of Technology, 9 Feb., 1989.

[9] National Computer Security Center, *Final Evaluation Report Boeing MLS LAN*, 21 June 1994.

[10] *Common IP Security Label*, Trusted Systems Interoperability group.

[11] Dan Schnackenberg, *Applying the Orange Book to an MLS LAN*, Proceedings of the 10th National Computer Security Conference, September 1987.

[12] Michelle J. Gosselin, *The Development of a Low-to-High Guard*, 14th National Computer Security Conference, Washington, D.C., 1991.